EU'S DATALAGRINGSDIREKTIV

RETTSLIGE KONSEKVENSER AV EN GJENNOMFØRING AV DIREKTIVET I NORSK RETT

Kandidatnummer: 691

Leveringsfrist: 25.11.09

Til sammen 16 675 ord

18.06.2010

Innholdsfortegnelse

1 Innledning og avgrensninger

1.1 Innledning

Den 15. mars 2006 ble direktiv 2006/24/EF, kjent som datalagringsdirektivet, vedtatt i EU. Direktivet trådte i kraft innenfor EU den 15. september 2007, jf. art. 15[1].

Ved ikrafttredelse av direktivet ble det innført en plikt til lagring av trafikkdata for tilbydere av elektronisk kommunikasjonstjenester[2]. Formålet for lagringen skal være bekjempelse av grov kriminalitet[3]. Direktivet angir spesifikt hvilke type opplysninger som skal lagres[4], og samtidig reguleres lagringstiden for trafikkdataopplysningene[5].

På grunn av Norges medlemskap i EØS, kan det være aktuelt å gjøre datalagringsdirektivets innhold til norsk rett.

Avhandlingen min tar for seg forskjellene mellom EU's datalagringsdirektiv og norske rettsregler på området og hvilke minimumsendringer som må til i vårt lovverk for å oppfylle Norges forpliktelser overfor EØS. Hovedspørsmålet bli om det må store endringer til i norsk rett for å gjennomføre direktivets innhold. Videre tar jeg stilling til hvorvidt eksisterende personvernregler stenger for en innføring av datalagringsdirektivets bestemmelser.

---

[1] Dog kunne medlemslandene velge en utsatt ikrafttredelse for deler av direktivet frem til 15. mars 2009.

[2] Jf. direktivets art. 3.

[3] Jf. art. 1, samt fortalen.

[4] Jf. art. 5

[5] Jf. art. 6

1.2 Oppbygning av oppgaven

For å belyse temaet for oppgaven, tar jeg for meg direktivets regler enkeltvis, og fremstiller innholdet av disse. Direktivet innebærer at det blir spørsmål om rettsendring innenfor fire hovedpunkter: hvilke opplysninger som skal lagres, formålet med lagringen, hvor lenge opplysningene skal oppbevares, samt at det ved direktivet vil skje en overgang fra sletteplikt til lagringsplikt for tilbydere av tele- og internettjenester. Hovedtyngden av oppgaven legges på lagringens innhold og formålsbestemmelsen. Det er her det reiser seg flest interessante problemstillinger. Reglene om innføring av lagringsforpliktelse og tidsperiode behandler jeg forholdsvis kort.

Jeg legger opp avhandlingen min etter disse fire punktene. Som første del, kapittel 3, drøftes innholdet av lagringsplikten. Her redegjør jeg for hvilke opplysninger som skal lagres i henhold til datalagringsdirektivet. Dette er et tungt og teknisk emne, men det er nødvendig at leser setter seg godt inn i temaet før de øvrige emnene drøftes. Det er her direktivets rekkevidde avklares, og det er kun for disse opplysningene resten av direktivet får relevans. I kapittel 4 tar jeg for meg innføringen av lagringsforpliktelsen, kapittel 5 omhandler lagringens formål, og i kapittel 6 fremstilles reglene om lagringstid.

Jeg foretar fortløpende en fremstilling av gjeldende norsk rett tilknyttet disse fire emnene, og avslutningsvis i hvert kapittel sammenliger jeg regelsettene og konkluderer med hvilke krav til endringer direktivet stiller.

I kapittel 7 drøfter jeg det menneskerettslige synet på endringene. Aktuell hjemmel er Den europeiske menneskerettskonvensjon art. 8 som omhander menneskets rett til vern av sin personlige frihet.

Kapittel 8 gir en oppsummering og konklusjon på det jeg har funnet frem til i prosessen. Her tillater jeg meg å komme med råd i forhold til gjennomføring av direktivet i norsk rett.

1.3 Avgrensninger

Jeg har for det første valgt å ikke ta for meg problemstillingen som er reist rundt datalagringsdirektivets forhold til EØS, og dermed hvorvidt Norge i det hele tatt skal være forpliktet til å gjennomføre direktivet som følge av EØS-samarbeidet. Det har vært stilt spørsmål rundt direktivets hjemmel i EU-regelsettet, noe som videre innebærer en uvisshet rundt dets rolle for EØS-medlemslandene. Jeg har satt som forutsetning i min videre drøftelse at direktivet er EØS-relevant. Som en del av dette spørsmålet hører Norges mulighet til å velge å ikke gjennomføre direktivet gjennom veto, selv om det skulle vise seg at direktivet hører under søyle 1 og dermed er en del av EØS-samarbeidet. Dette vil jeg heller ikke ta stilling til.

Selv om det skulle vise seg at datalagringsdirektivet ikke er EØS-relevant, kan det likevel være aktuelt med lignende lovregler i Norge. Terrortrusselen, som er anført i direktivets fortale[6], kan gjøre seg sterkere gjeldende også her i landet. Flere europeiske land så behovet for en lagringsplikt for opplysninger om elektronisk kommunikasjon allerede før spørsmålet kom opp på et internasjonalt nivå[7]. Ulikheter mellom de reguleringer som da ble gitt i EU-land var begrunnelsen for at EU så seg nødt til å gi reguleringer for å få et harmonisert regelverk innenfor Fellesskapet.

Jeg har videre valgt å avgrense i forhold til den praktiske gjennomføring av lagringsplikt for trafikkdata. Artikkel 7 til 9 i datalagringsdirektivet inneholder regler om databeskyttelse og datasikkerhet. Disse bestemmelsene innebærer et krav til endring av norske regler, men jeg har valgt å ikke drøfte dette. Det samme gjelder art. 10 som omhandler statistikk over lagring av data.

[6] Se direktivets fortale punkt (8)

[7] Se direktivets fortale punkt (5)

2 Direktiv 2006/24/EF – Datalagringsdirektivet

2.1 Historikk

Den viktigste rettskilden for denne avhandlingen er EU's datalagringsdirektiv – direktiv 2006/24/EF. Nedenfor følger en kort historikk for direktivets tilblivelse og en oversikt over reglene for å gi en innsikt i og forståelse for dets innhold.

For å kunne se spørsmålene som reiser seg i deler av oppgaven, er det viktig å være klar over at behandling av opplysninger om elektronisk kommunikasjon har vært et tema innenfor EU-retten i flere år. En prosess for å styrke individers personvern startet i 1995. Da kom spørsmålet om behandling av personlige opplysninger opp i EU-fellesskapet gjennom direktiv 95/46/EF, kjent som EU's personverndirektiv. Direktivet omhandler beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger. Som følge av Norges EØS-forpliktelser ble personverndirektivet gjennomført som norsk lov i personvernloven, lov av 31. mars 2000 nr. 31. Fysiske personers rett til vern av privatlivets fred står i sentrum for reguleringene, og det settes derfor vilkår for behandling av personopplysninger jf. legaldefinisjonen i § 2.

I 1997 kom telekommunikasjonsdirektivet som et utdyping av personverndirektivet fra 1995, direkte rettet mot telekombransjen. Artikkel 6 nr. 1 behandlet adgangen til lagring av trafikkdata vedrørende abonnentene eller brukerne, og medførte sletteplikt når det gjaldt trafikkopplysninger. Direktivet innebar en styrking av personvernet.

I 2002 ble kommunikasjonsverndirektivet, direktiv 2002/58/EF, vedtatt i EU. Herved ble det gitt spesialreguleringer for behandling av personopplysninger og beskyttelse av privatlivets fred innenfor elektronisk kommunikasjonssektor. Sletteplikten ble opprettholdt for "trafikkdata", jf. art. 6 nr. 1. Direktivet er gjennomført i Norge gjennom lov om

elektronisk kommunikasjon av 4. juli 2003 nr. 83 (ekomloven). Telekommunikasjonsdirektivet ble samtidig satt ut av kraft.

Etter dette utviklet rettstilstanden seg innenlands i Europa, blant annet innførte Danmark i 2002 bestemmelser i Retsplejeloven[8] som påla loggingsplikt for tele- og internettilbydere. Utviklingen medførte en uoverensstemmelse mellom sletteplikt i enkelte EU-land og lagringsplikt i andre, samt ulikheter innenfor de ulike reguleringene. Tele- og internettbransjen er en sektor hvor det skjer omfattende samarbeid over landegrensene. Daglig skjer en enorm utveksling av trafikkdata mellom europeiske land. Telefonsamtaler finner sted mellom brukere som befinner seg i ulike deler av Europa, og jevnt foretas det oppkobling til internettsider med opphav i andre land enn brukerens tilholdssted.

Som følge av ulik lovgivning i Europa med hensyn til lagring av elektronisk kommunikasjon, så EU seg nødt til å gi nye bestemmelser som ville bryte med den tidligere sletteplikten. At det ble stilt forskjellige krav til tjenestetilbyderne ut ifra hvilket land de opererer i medførte, ifølge EU, hindringer i den frie flyt av tjenester[9]. En av hovedbegrunnelsene for EU-samarbeidet er at tjenestetilbydere innenfor Fellesskapet skal behandles likt. Dersom internettilbydere får ulike regler å forholde seg til etter hvor de har etablert seg innenfor EU, opprettholdes ikke denne likheten. For å motvirke utviklingen, var det nødvendig med regelharmonisering i Fellesskapet. Med denne bakgrunn ble Datalagringsdirektivet vedtatt. Regelharmonisering som formål følger av direktivets artikkel 1. I tillegg er begrunnelsen fremhevet i direktivets fortale punkt 5 og 6.

Datalagringsdirektivet innebærer at alle tilbydere av elektroniske tjenester innenfor EU har en forpliktelse[10] til å lagre nærmere angitte trafikkdata knyttet til sine brukere[11] for en

[8] § 786, 4. ledd

[9] Se EF-traktaten art 49

[10] Jf. art 3 nr. 1

[11] Jf. art. 5

periode på minimum seks måneder og maksimalt to år[12]. Dette er opplysninger som gjelder fasttelefoni, mobiltelefoni og internettbruk, herunder e-post og telefoni via internett[13]. Datalagringsdirektivet regulerer lagring av opplysninger vedrørende fysiske og juridiske brukere, jf. artikkel 1 nr. 2. Utover valgfriheten når det gjelder lagringstid[14], etterlates intet rom for medlemslandene til å foreta reguleringer i uoverensstemmelse med direktivet.

Når en ser på direktivets historie, kan en spørre seg om reglene om lagringsplikt kom som følge av kritikk av sletteplikreglene i de tidligere direktiver. Ville det i det hele tatt kommet på tale med reguleringer om lagringsplikt dersom det ikke tidligere hadde blitt vedtatt bestemmelser om at trafikkdata skulle slettes?

Reglene om sletteplikt som kom i direktivene fra 1997 og 2002 innebar samtidig en mulighet til lagring av trafikkdata så fremt de kunne anses å være nødvendige i forhold til formålet[15]. Dette innebar at det til en viss grad var opp til tilbyderne å velge om de ønsket å oppbevare disse opplysningene, noe de gjerne ønsket for å ha bevis for kundenes bruk og unngå fremtidige tvister om fakturabeløp. Direktivene medførte for tilbyderne en begrensning i muligheten til oppbevaring av kundeopplysninger, og de ønsket trolig å kunne oppbevare opplysninger om kundenes telefoni og databruk i langt større grad enn det direktivene åpnet for. Bestemmelsene som kom skulle styrke personvernet for individene, og tok ikke hensyn til tilbydernes ønsker. Kan en dermed si at datalagringsdirektivets historikk har blitt dets egen fiende?

En kan tenke seg at dersom operatørene ikke fra først av hadde blitt pålagt å slette trafikkdata knyttet til sine kunder, hadde det aldri vært behov for å gi reguleringer om deres plikt til å lagre de samme opplysningene. Situasjonen hadde regulert seg selv, som en konsekvens av tilbydernes valgfrihet når det gjaldt lagring av opplysninger i egen interesse,

[12] Jf. art 6

[13] Jf. art. 5

[14] Se kapittel 6

[15] Se personverndirektivet art. 7 og kommunikasjonsverndirektivet art. art. 6 nr. 2

innenfor rammen av nødvendighetsprinsippet. Når reglene om lagringsplikt nå er innført i EU-samarbeidet, føles de i bransjen som et tvangsmessig grep, brukt for å tilfredsstille andre behov i samfunnet. En påtvunget plikt som stiller nye krav til lagringsplass og innebærer omlegging av rutiner. Dette er kanskje årsaken til at mange på tilbydersiden uttrykker skepsis til de nye reglene.

2.2 Norges forpliktelser etter EØS-avtalen

Jeg har, som nevnt i punkt 1.3, valgt å avgrense oppgaven mot direktivets EØS-relevanse, et spørsmål som dreier seg om EØS-samarbeidets forhold til EU. I dette kapittelet redegjør jeg derimot for Norges forhold til EØS, som er et annet spørsmål. Spørsmålet reiser seg i forbindelse med Norges internasjonale forpliktelse til å gjøre datalagringsdirektivets innhold til norsk rett. Denne juridiske forpliktelsen følger av EØS-avtalen, som Norge inngikk i 1992, med virkning fra 1. januar 1994[16].

EØS-loven gjennomfører EØS-avtalen i norsk rett, jf. § 1. Etter EØS-avtalen art. 7 skal rettsakter som inntas som vedlegg til EØS-avtalen være bindende for avtalepartene og gjøres til endel av deres interne rett. Norge er dermed juridisk forpliktet overfor EØS til å gjennomføre datalagringsdirektivet. At vi har å gjøre med et direktiv, innebærer at dets innhold skal gjennomføres med den form og de midler norske myndigheter bestemmer, se EØS-avtalen art. 7, bokstav b).

2.3 Gjennomføring av datalagringsdirektivet

Spørsmålet blir da hvordan datalagringsdirektivet skal gjennomføres i norsk rett. Dette er det opp til norske myndigheter å avgjøre, jf. EØS-avtalen art 7. Med andre ord kan Norge velge å vedta en ny lov hvor datalagringsdirektivet gjengis i en ordrett oversettelse, eller gjennomføre de endringene direktivet vil innebære enkeltvis i de lovene som regulerer lagring av trafikkdata i dag.

[16] Jf. eøs-loven § 7

Velges det første alternativet, er vi forsikret om at alle Norges forpliktelser etter datalagringsdirektivet oppfylles overfor EØS. Da må det imidlertid spørres om vi samtidig trenger å endre gjeldende regler på området. Prioritetsprinsippet Lex Posterior innebærer at "nyere regler har fortrinn fremfor eldre"[17]. Dermed vil bestemmelser i en "datalagringslov" gå foran, slik at bestemmelser i eldre lovgivning må vike. Denne motstridsregelen er imidlertid på ingen måte ufravikelig, og for å være helt sikker på at bestemmelsene som gjennomfører datalagringsdirektivet ikke skal bli tilsidesatt av tidligere regler, bør disse derfor endres. Det mest elegante er også at regelverket stemmer overens, og hvertfall ikke står i direkte motstrid til hverandre.

Det andre alternativet er at Norge velger en enkeltvis endring i de regler som per i dag finnes på området, slik at disse samlet sett sørger for at Norge oppfyller sine EØS-rettslige forpliktelser etter datalagringsdirektivet. Dette vil være en ryddig fremgangsmåde, idet "dobbeltreguleringer" unngås. Dersom datalagringsdirektivet vil medføre kun små endringer, kan dette være den enkleste måten å sørge for en gjennomføring av direktivet.

Spørsmålet om hvilket av disse alternativer som er å foretrekke tar jeg stilling til i kapittel 8, etter at jeg har konkludert med hvilke endringer datalagringsdirektivet totalt sett vil innebære for norsk rett.

2.4 Sammenligningsgrunnlag – hvilke norske lover kan være relevante?

2.4.1 Personopplysningsloven med tilhørende forskrift og standard konsesjon

Et naturlig utgangspunkt for å undersøke hva som gjelder for lagring av trafikkdata i Norge idag, er lov av 31. mars 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven).

[17] Eckhoff (2001) s. 348

Loven regulerer ”behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler”, jf. § 3, første ledd a). Hva som anses som en ”personopplysning”, defineres i lovens § 2 nr. 1):

> ”personopplysning: opplysninger og vurderinger som kan knyttes til en enkeltperson”.

Datalagringsdirektivet regulerer som vist ovenfor[18] lagring av opplysninger om kunders bruk av telefon og internett. Dette er opplysninger som potensielt kan falle innenfor personopplysningslovens definisjon av ”personopplysninger”. I vårt tilfelle vil det da måtte dreie seg om behandling av opplysninger som direkte kan knyttes til en bruker av telefon- eller internettjenester. Derfor vil det være naturlig å undersøke personopplysningslovens bestemmelser nærmere når en skal foreta en sammenligning mellom datalagringsdirektivets innhold og norsk rett. Personopplysningslovens bestemmelser regulerer kun lagring av opplysninger som gjelder fysiske personer. Det vil si at lagring av opplysninger om trafikkdata knyttet til juridiske personer faller utenfor lovens regler[19]. Dermed overlapper ikke datalagringdirektivet og personopplysningsloven hverandre fullstendig. Hvorvidt datalagringsdirektivet og personopplysningsloven ellers har sammenfallende virkeområder, finner vi først ved en gjennomgang av lovverkene og hvilke opplysninger de regulerer lagring av. En slik gjennomgang foretar jeg i kapittel 3. Først når jeg i kapittel 3 har tatt for meg hvilke opplysninger som skal lagres etter datalagringsdirektivet, kan jeg konkludere med om personopplysningsloven har det samme virkeområdet som direktivet, eventuelt ved hvilke former for lagring regelsettene overlapper hverandre, slik av de kan brukes til sammenligning.

Personopplysningsloven utfylles av reguleringer gitt i personopplysningsforskriften[20] og ”Konsesjon til å behandle personopplysninger – behandling av opplysninger om

---

[18] Punkt 2.1.

[19] Schartum (2004) s 108

[20] Forskrift 2000.12.15 nr. 1265

abonnenters bruk av teletjenester" med kommentarer, utformet av Datatilsynet med hjemmel i personopplysningsforskriften[21].

2.4.2 Lov om elektronisk kommunikasjon med forskrift

I tillegg til Personopplysningsloven inneholder lov av 4. juli 2003 nr. 83 om elektronisk kommunikasjon[22] viktige reguleringer om lagring av kundeopplysninger.

Loven gjelder "virksomhet knyttet til overføring av elektronisk kommunikasjon"[23], hvor "elektronisk kommunikasjon" defineres i ekomloven § 1-5 nr. 1 som "Overføring av lyd, tekst, bilder eller andre data ved hjelp av elektromagnetiske signaler i fritt rom eller kabel...". Ekomloven omfatter med andre ord virksomhet knyttet til tele- og internettjenester.

For å få en full oversikt over norske regler om lagring av kundedata, må altså også ekomloven undersøkes nærmere.

I motsetning til personopplysningsloven regulerer ekomloven også opplysninger om bruker som er juridisk person i tillegg til fysiske personer, jf. § 1-5 nr. 12. For øvrig avgjøres også her virkeområde først etter en nærmere gjennomgang av reglene i loven. Dette gjør jeg under punkt 3.2.2 og 3.3.2 nedenfor.

2.4.3 Forholdet mellom Personopplysningsloven og Ekomloven.

Ettersom både personopplysningsloven og ekomloven regulerer tilbyders plikt til å slette opplysninger knyttet til bruk av tele- og internettjenester, reises det spørsmål om hvilke saksområder som plasseres under den enkelte lov og hvilken lov som dermed skal anføres

[21] Se forskriften § 7-1

[22] Heretter Ekomloven

[23] Jf. § 1-2

som hjemmel for sletteplikt og lagringsadgang. Dette er av betydning også for å avgjøre hvor eventuelle nye reguleringer skal gjennomføres.

Personopplysningsloven regulerer ”personopplysninger”, og angir en sletteplikt for disse i § 28:

> ”Den behandlingsansvarlige skal ikke lagre personopplysninger lenger enn det som er nødvendig for å gjennomføre formålet med behandlingen. Hvis ikke personopplysningene deretter skal oppbevares i henhold til arkivloven eller annen lovgivning, skal de slettes.”

Ekomloven pålegger tilbyderne å slette ”trafikkdata” jf. § 2-7, annet ledd:

> ”Trafikkdata skal slettes eller anonymiseres så snart de ikke lenger er nødvendig for kommunikasjons- eller faktureringsformål, med mindre annet er bestemt i eller i medhold av lov.”

Det er ikke gitt at ”personopplysninger” og ”trafikkdata” omfatter de samme kundeopplysningene, slik at disse bestemmelsene kan sies å ha det samme omfanget. For å avgjøre dette, må en se nærmere på disse uttrykkene.

Definisjonen på ”personopplysning” er gitt i personopplysningsloven § 2 nr. 1) og omfatter ”opplysninger og vurderinger som kan knyttes til en enkeltperson”.

Ekomloven inneholder ingen definisjon av ”trafikkdata”. Det finner vi derimot i ekomforskriften § 7-1, første ledd, annet punktum. Uttrykket er vidt definert og omfatter alle data som er ”nødvendig for å overføre kommunikasjon i et elektronisk kommunikasjonsnett eller for fakturering av slik overføring”. Sammenligner vi denne definisjonen med ordlyden i ekomloven § 2-7, annet ledd, ser vi at de er veldig like. Ekomloven § 2-7, annet ledd bestemmer at trafikkdata skal slettes når de ”ikke lenger er nødvendig for kommunikasjons- eller faktureringsformål”. Ved en nærmere studie av disse bestemmelsene, ser vi at ekomloven § 2-7, annet ledd innebærer at ”trafikkdata” skal slettes når de ikke lenger er ”trafikkdata”. Hvorvidt data er ”nødvendig for kommunikasjons- eller

faktureringsformål" avgjør altså både om de kan defineres som "trafikkdata" og omfattes av ekomloven § 2-7, annet ledd og hvor lenge de kan lagres etter denne bestemmelsen. Det innebærer at tidsangivelsen for lagringsadgangen i bestemmelsen egentlig blir uten innhold. Er opplysningene ikke lenger "nødvendig for kommunikasjone- eller faktureringsformål", er de heller ikke "trafikkdata", og omfattes ikke av bestemmelsen i utgangspunktet!

Forarbeidene til ekomloven inneholder den samme definisjonen av "trafikkdata", men her finner vi også eksempler på hva som kan være slike data: "Med trafikkdata menes f.eks. data som angir kommunikasjonens opphavssted, bestemmelsessted, rute, klokkeslett, dato, omfang, varighet og underliggende tjeneste"[24].

"Trafikkdata" er antatt av personvernkommisjonen å være "personopplysninger"[25]. Dette er data som ofte, dog ikke alltid, kan knyttes til enkeltpersoner. Dermed vil ikke "trafikkdata" ha et videre innhold enn "personopplysninger". Det kan med andre ord ikke tenkes at vi har opplysninger som kun faller inn under ekomloven og ikke samtidig per definisjon under personopplysningsloven. Det motsatte kan imidlertid tenkes. Data som faller inn under definisjonen av "personopplysning", trenger ikke nødvendigvis å være "trafikkdata" som reguleres av ekomloven. Definisjonen av "personopplysning", jf. personopplysningsloven § 2 nr. 1 er vid, og omfatter opplysninger som ikke har tilknytning til bruk av tele- og internettjenester. Også i vår sammenheng kan det være aktuelt med opplysninger som kan knyttes til bruker av disse tjenester, men ikke nødvendigvis går inn under definisjonen av "trafikkdata". Dette ser vi etter gjennomgang av de ulike opplysningene datalagringsdirektivet regulerer, jf. kapittel 3 nedenfor.

Eventuelle "personopplysninger" som ikke kan regnes som "trafikkdata" reguleres naturlig nok kun av personopplysningsloven. I de tilfeller hvor opplysningene omfattes av definisjonen av "trafikkdata", og dermed også regnes som "personopplysning", er det ikke

[24] Se Ot.prp. nr. 58 (2002-2003) s. 92

[25] Se NOU 2009: 1 s. 193

klarert hvilken lov som skal følges. Skal ekomloven eller personopplysningsloven anføres som hjemmel?

Der bruker er juridisk person, vil ikke personopplysningsloven komme til anvendelse[26]. Det vil derimot ekomloven, som ikke har en tilsvarende begrensning i anvendelsesområde[27]. Dermed vil en opplysning som regnes som "trafikkdata", og som også i utgangspunktet er en "personopplysning", men som er knyttet til en juridisk person, kun følge ekomlovens bestemmelser.

Der brukeren er en fysisk person er det mer uklart hvilken lov som gjelder for lagring og sletting av opplysninger vedrørende dennes tele- og internettbruk, og som skal anføres som hjemmel. "Trafikkdata" faller da som utgangspunkt inn under begge lovene. I ekomloven § 2-7 gjøres det forbehold for annen lovgivning, noe som kan tolkes derhen at personopplysningsloven likevel skal være gjeldende for fysiske personer. Av Personopplysningsloven § 5 følger derimot at annen "særskilt lov som regulerer behandlingsmåten" skal gå foran bestemmelsene i denne loven. Ekomloven vil typisk være slik annen lov. Dermed står saken uavklart så langt. Tele- og internettselskapene får sin konsesjon for behandling av slike opplysninger fra Datatilsynet, med hjemmel i personopplysningsforskriften. Dette tyder på at oppfatningene i bransjen er at det er denne loven som gjelder. Denne forskriften, som er gitt etter personopplysningsloven, må riktignok være "annet som er bestemt i eller i medhold av lov" som går foran bestemmelsen i ekomloven § 2-7. Ekomloven er en lov som først og fremst skal "sikre brukerne i hele landet gode, rimelige og fremtidsrettede elektroniske kommunikasjonstjenester", jf. § 1-1. Personopplysningslovens hovedformål er "å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger". Etter lovenes formål er det derfor også nærliggende å gi personopplysningsloven § 28 forrang fremfor ekomloven § 2-7.

[26] Se punkt 2.4.1

[27] Jf. § 1-5 nr. 12

Personopplysningslovens gjennomføring ligger under Datatilsynet[28], mens det er Post- og teletilsynet som har myndighet etter ekomloven[29]. Det fremstår som naturlig at det er under Datatilsynets virke å gi konsesjon for behandling av opplysninger av personlig art. Post- og teletilsynets rolle er stort sett knyttet til fordeling av frekvenser og lignende, mer av teknisk art. Datatilsynet har derimot ekspertise innenfor personvern. Lex specialis-prinsippet står imidlertid sterkt i vår sammenheng. Lex specialis-prinsippet medfører at ekomlovens bestemmelser går foran tilsvarende regler i personopplysningsloven[30]. Ekomloven er en særlov som gjelder for elektronisk kommunikasjon, mens personopplysningsloven gjelder behandling av personlige opplysninger generelt[31].

Konklusjonen må nok derfor bli at ekomloven kommer til anvendelse og skal anføres som hjemmel for behandling av "trafikkdata", både når opplysningene kan knyttes til juridiske og fysiske personer. En lagringsplikt bør derfor hjemles i ekomloven når det gjelder "trafikkdata". I tillegg må personopplysningslovens øvrige bestemmelser kunne anvendes på "trafikkdata" som gjelder fysiske personer. Videre må personopplysningsloven gjelde for øvrige "personopplysninger" som ikke omfattes av definisjonen på "trafikkdata".

[28] Se personopplysningsloven kap. VIII, herunder § 42, tredje ledd.

[29] Se ekomloven § 1-4.

[30] Det samme følger av lex posterior-prinsippet.

[31] Jf. definisjonen i § 2 nr. 1

3 Lagringspliktens innhold – hvilke opplysninger skal lagres?

3.1 Innledning

3.1.1 Datalagringsdirektivet

Datalagringsdirektivet innebærer en lagringsplikt for "data"[32] tilknyttet bruker av elektronisk kommunikasjonstjeneste. "Data" er definert i art. 2 nr. 2 a) og omfatter "trafikkdata, lokaliseringsdata og lignende data som er nødvendige for å identifisere abonnenten eller brukeren".

Datalagringsdirektivets artikkel 5 konkretiserer hvilke opplysninger som skal lagres av tilbyder. Bestemmelsen angir spesifikt hvilke opplysninger som skal lagres, og derfor må den karakteriseres som uttømmende, slik at andre typer opplysninger enn de som er nevnt, ikke er gjenstand for lagring. Ettersom lagring av personlige opplysninger er å anse som inngrep, innebærer legalitetsprinsippet at lagringen må hjemles i lov, slik at det blir mindre rom for analogi og utvidende tolkinger[33].

Art. 5 skiller mellom 1) data som gjelder fasttelefoni og mobiltelefoni og 2) data som gjelder internettbruk og e-post og telefoni via internett. Datalagringsdirektivet angir altså spesifikt hvilke kommunikasjonsformer lagringsplikten gjelder for. Det kan spørres om det utgjør et problem at det er kommunikasjonsnøytralt. For det første kan problemet anføres overfor alternative kommunikasjonsformer som eksisterer idag og som ikke omfattes av datalagringsdirektivets bestemmelser. Et eksempel på dette er satelittelefoni. Denne måten å kommunisere på er ikke nevnt i direktivet, og det må da antas at data knyttet til satelittelefoni ikke er underlagt lagringsplikten. Sammenholdt med datalagringsdirektivets

[32] Jf. art. 3, se nærmere i kapittel 4 nedenfor.

[33] Eckhoff (2001) s. 127

formål, bekjempelse av grov kriminalitet, innebærer dette en svakhet for direktivet. Kriminalitet kan gjennomføres via satelittelefon uten at det skjer noen form for lagring av kommunikasjonen som skjer, og dermed uten at påtalemyndighetene senere kan spore den aktiviteten som har skjedd.

Det samme spørsmålet må stilles når det gjelder fremtidige kommunikasjonstyper. Det kan meget godt tenkes at det utvikles nye former å kommunisere på i fremtiden. Hva vil da måtte skje med datalagringsdirektivet? Må det utvides for også å gjelde disse nye kommunikasjonsformene? For at direktivet best skal kunne oppfylle formålet med lagringsplikten, kreves det at datalagringsdirektivet stadig oppdateres med endringer og utvidelser slik at nye kommunikasjonsformer skal omfattes. Videre må endringene gjennomføres i nasjonal lovgivning for å få virkningskraft overfor tilbyderne. Dette er en tungvint fremgangsmåte, som innebærer tidsmessige ulemper. Lagringsplikt for trafikkdata knyttet til nye former for kommunikasjon forsinkes tilsvarende den tid prosessen tar.

Alternativet var å gi rundere, kommunikasjonsnøytrale bestemmelser, slik at også annen kommunikasjon enn fasttelefoni, mobiltelefoni, internett, telefoni og e-post via internett kunne innfortolkes i direktivet. Dette er kanskje heller ingen heldig løsning, når en ser på EU's begrunnelse for datalagringsdirektivet, nemlig harmonisering av medlemslandenes lagringsreguleringer. Ved å gi uklare bestemmelser ville det på nytt kunne oppstått ulik praksis i de forskjellige EU-landene, noe direktivet nettopp skulle sette en stopper for.

Norge kan velge å bruke videre begreper i sine gjennomføringsregler for å fange opp nåtidige og fremtidige alternative kommunikasjonsmåter, og sikre seg at disse blir regulert i samsvar med datalagringsdirektivet. Jeg har imidlertid forutsatt[34] en minimumsendring i norsk rett, og dermed oppfylles direktivets krav ved et tilsvarende ordvalg som ikke tar høyde på å omfatte andre former for kommunikasjon.

[34] Jf. punkt 1.1

3.1.2 Norsk rett

Hvilke opplysninger tilbydere av tele- og internettjenester i Norge kan loggføre i dag, bestemmes av ekomloven § 2-7, annet ledd og personopplysningsloven § 28.

Det må avgjøres konkret hvorvidt en opplysning er å anse som "personopplysning" og/eller "trafikkdata", for å fastslå hvilken lov som gjelder. Data som omfattes av definisjonen av "trafikkdata", reguleres av ekomloven og omfatter både fysiske og juridiske personer[35]. I min videre drøftelse nedenfor er det da naturlig å først konkludere med hvorvidt en opplysning er "trafikkdata". Er den å anse som det, gjelder sletteplikten etter ekomloven § 2-7, annet ledd. Er opplysningen derimot kun å anse som en "personopplysning" jf. personopplysningsloven § 2 nr. 1, kommer personopplysningsloven, som bare gjelder fysiske personer, til anvendelse.

Spørsmålet blir videre, etter begge lovverk, hvilke type opplysninger som kan anses som "nødvendige". Nødvendighetsvilkåret går igjen i de to lovene, men innholdet av det er ikke nødvendigvis det samme. Etter konsesjon til å behandle personopplysninger punkt 2 er innholdet av det klargjort hva som ligger i nødvendighetskravet. Konsesjonen er gitt med hjemmel i personopplysningsloven § 31, fjerde ledd[36] og gjelder dermed for "personopplysninger". Ifølge konsesjonen er det opplysninger som er "nødvendige for gjennomføring og fakturering av tjenesten" som kan behandles av konsesjonshaveren. Opplysningene som lagres må med andre ord kun brukes til kundeadministrasjon, fakturering og gjennomføring av internett- og telefonitjenestene. Det samme følger av personopplysningsloven § 11 b), hvor det angis at personopplysningene kan "bare nyttes til uttrykkelig angitte formål som er saklig begrunnet i den behandlingsansvarliges virksomhet". Ifølge Datatilsynets kommentar til konsesjon til å behandle personopplysninger for telekommunikasjon må spørsmålet avgjøres konkret ved en

[35] Se punkt 2.4.3

[36] Jf. personopplysningsforskriften § 7-1

”kvalifisert vurdering av hvilke opplysninger som faktisk er nødvendige for å gjennomføre og fakturere tjenesten”[37].

I Ekomlovens regulering av hvilke opplysninger som kan lagres frem til sletteplikten inntrer, jf. art. 2-7, annet ledd, fremgår det hva som her skal være formålet med lagringen. Det sies klart at opplysninger kan lagres når de er ”nødvendige for kommunikasjons- eller faktureringsformål”.

Med andre ord må både”personopplysninger” og ”trafikkdata” være nødvendige for kommunikasjons- eller faktureringsformål for å kunne behandles (og dermed eventuelt lagres).

Faktureringsformålet vil innebære at tilbyderen kan lagre oppysninger som er nødvendige for å klargjøre fakturabeløpet. Opplysninger som er nødvendige for kommunikasjonsformål, vil typisk være hvem som er mottaker av en e-postforsendelse, helt til e-posten når frem til denne. Når e-posten er kommet frem til bestemmelsesstedet, har tilbyderen ikke lenger behov for mottakerens e-postadresse for å gjennomføre tjenesten.

3.1.3 Oppbygning videre

I den videre fremstilling skiller jeg mellom lagring av opplysninger som gjelder kundens bruk av teletjenester under punkt 3.2 og bruk av internettjenester under punkt 3.3.
Under punkt 3.2.1 og 3.3.1 redegjør jeg for datalagringsdirektivets bestemmelser om hvilke opplysninger som skal lagres, og under punkt 3.2.2 og 3.3.2 gjennomgår jeg norsk rett slik den er idag. For oversiktens skyld har jeg valgt å foreta en fortløpende sammenligning med datalagringsdirektivet i fremstillingen av norsk rett, hvor jeg knytter drøftelsen direkte opp mot datalagringsdirektivets bestemmelse om hvilke opplysninger som skal lagres. Eventuelle andre ”personopplysninger” eller ”trafikkdata” som kan behandles etter norsk rett idag er ikke interessant for denne avhandlingens tema.

[37] Kommentaren s. 1

Under punkt 3.4 Endring/sammenligning trekker jeg ut endringene jeg har kommet frem til og drøfter dem mer gjennomgående. Der konkluderer jeg med hvilke lovendringer som kreves for å gjennomføre datalagringsdirektivets innhold.

3.2 Telefoni

3.2.1 Datalagringsdirektivet

3.2.1.1 Data som sporer og identifiserer kilden til kommunikasjonen

For det første innebærer direktivet en plikt til å lagre opplysninger som skal kunne benyttes til å "spore og identificere kilden til en kommunikation", jf. art. 5 nr. 1. a). Brukerens A-nummer er sentralt for denne identifisering, og skal lagres etter art. 5 nr. 1 a) 1) i). A-nummeret er det telefonnummer som er tilknyttet tilbydernes enkelte brukere, og som disse benytter seg av når de foretar utgående telefonsamtaler.

Videre skal brukerens navn og adresse oppbevares, jf. art. 5 nr. 1 a) 1) ii). Disse opplysningene er viktige for å kunne knytte telefonibruken til en bestemt kunde.

3.2.1.2 Data som fastslår kommunikasjonens bestemmelsessted

I tillegg til opplysninger som gjelder brukeren, kommer opplysninger som skal fastslå bestemmelsesstedet for kommunikasjonen. Hjemmel for lagring av disse opplysninger er art. 5 nr. 1. b) 1) i). Etter denne bestemmelsen skal alle B-numre lagres. Dette er de numre abonnenten har valgt for sin oppringning, sms-forsendelse osv. Herunder omfattes også numre han viderekobles til.

Navn og adresse til brukeren av b-nummeret skal også lagres, jf. art. 5 nr. 1. b) 1) ii).

3.2.1.3 Data som fastslår en kommunikasjons dato, klokkeslett og varighet

Etter art. 5 nr. 1. c) 1) skal tilbyderne lagre opplysninger som gjelder tidspunktet for telefonikommunikasjonen. Dato og klokkeslett for både begynnelse og avslutning av kommunikasjonen skal registreres og lagres.

3.2.1.4 Data som identifiserer kommunikasjonstypen

Med hjemmel i art. 5 nr. 1 d) 1) skal det også lagres opplysninger for å identifisere kommunikasjonstypen. Dette innebærer hvorvidt brukeren har benyttet sin telefon til oppringning, sms, mms osv.

3.2.1.5 Data som identifiserer brukerens kommunikasjonsutstyr

Art. 5 nr. 1 e) 1) og 2) gir bestemmelser om lagring av opplysninger som skal identifisere "brugernes kommunikationsudstyr eller det, der fremstår som værende deres udstyr".

For fasttelefoni innebærer dette A-nummer og B-nummer, jf. 1). For mobiltelefoni skal det foruten A- og B-nummer lagres A-abonnentens og B-abonnentens IMSI-nummer og IMEI-nummer, jf. 2) i) –v).

IMSI er en forkortelse for «International Mobile Subscriber Identity»[38]. Til hvert SIM-kort er det tilknyttet et IMSI-nummer som brukes til identifisering av brukerne ved internasjonale oppringninger. Et A-nummer er ikke tilstrekkelig til idenfikasjon av brukeren dersom telefonen brukes utenlands, derfor må også IMSI-nummeret registreres, for å gjøre det mulig å knytte kommunikasjonen til riktig abonnent.

IMEI-nummeret er et nummer som identifiserer telefonen som er brukt. Hver mobiltelefon er utstyrt med et unikt IMEI-nummer. Når en bruker foretar en oppringning fra mobiltelefon, registreres IMEI-nummeret av tilbyderen, slik at det kan fastslås hvilken

[38] Se Ot.prp nr. 58 2002-2003 s. 94

telefon som er brukt. Dette er opplysninger som kan være viktige i en videre oppsporing av hvem som har foretatt oppringningen. Det vil ikke være tilstrekkelig å kunne angi hvem som er registrert som bruker av A-nummeret for å kunne si at det er denne som har foretatt oppringningen.

Når det gjelder forhåndsbetalte anonyme tjenester av mobiltelefoni, skal det etter art. 5 nr. 1 e) 2) vi) lagres hvilket tidspunkt tjenesten for første gang ble aktivert og hvor denne aktiveringen ble foretatt (ved hjelp av celle-ID). Dette gjelder kontantkort som ikke registreres på person ved aktivering. I Norge er det imidlertid ikke lenger mulig å kjøpe kontantkort og ikke samtidig registrere dette til en person. Dette følger av ekomforskriften § 6-2, som sier at tilbyder skal føre oversikt over ”enhver sluttbrukers navn, adresse og nummer/adresse for tjeneste”.

3.2.1.6 Data som foretar en lokalisering av mobilt utstyr

Avslutningsvis skal også data som innebærer lokalisering av mobilt utstyr lagres etter art. 5 nr. 1. f).

Så lenge en mobiltelefon er påslått, vil den sende ut signaler til nærmeste basestasjon. Dette registreres, og medfører at en i ettertid kan gå tilbake og fastslå i hvilket område telefonen og sim-kortet (A-nummeret) har befunnet seg. Signalstyrken angir nærmere plasseringspunkt, og signalene fra de ulike mastene krysspeiles av samme årsak. Denne prosessen skjer selv om ikke telefonen er i bruk til oppringning eller sending av sms eller lignende.

Celle-ID angir det geografiske området for hvor telefonen befinner seg. Tilbydernes dekningsområde er delt inn i celler med hver sin identifikasjonskode, delt inn av radioplanleggere hos hver tilbyder. En celle kan bestå av flere basestasjoner som sender ut signaler og kommuniserer med telefonenes sim-kort. Hver tilbyder av teletjenester har sitt eget cellesystem/dekningskart.

Etter art. 5 nr. 1. f) 1) skal lokaliseringskoden ved kommunikasjonens begynnelse lagres. Hva dette innebærer, har sammenheng med hva som menes med ”kommunikasjon”. Er dette en angivelse av når mobiltelefonen begynner å kommunisere med basestasjonen, eller når det startes kommunikasjon til en annen bruker via oppringning, sms eller lignende? Medfører dette at lokaliseringen lagres hele tiden mens telefonen er slått på, eller at det bare lagres hvor telefonen/simkortet befinner seg mens den er i bruk?

Et første alternativ vil medføre at en enorm mengde data må lagres av tilbyderne. Det vil da måtte lagres hvor enhver bruker befinner seg til enhver tid av døgnet mens telefonen hans er påslått. Et alternativ hvor loggføring kreves kun mens telefonen er i bruk innebærer også at en mengde data må lagres av tilbyder, men i langt mindre grad enn alternativ nr. 1.

Ut i fra en naturlig språklig forståelse, er det mest sannsynlig at det menes kommunikasjon med en annen bruker via ulike teletjenester. Dette er også i tråd med ordlyden i resten av direktivet, hvor kommunikasjon er brukt i denne sammenheng, og ikke som kommunikasjon mellom tekniske enheter. Kommunikasjon med basestasjonene er en mer søkt tolking av uttrykket, og må være nærmere utdypet i lovteksten for å kunne sies å være gjeldende rett. Denne konklusjonen støttes også opp av hensynet til forutberegnelighet.

Det må derfor være kommunikasjon via telefonbruk som igangsetter lagring av hvor brukeren befinner seg. Dermed vil det ikke blir loggført hvor brukeren befinner seg så lenge telefonen er påslått, men ikke i bruk.

Art. 5 nr. 1. f) 2) innebærer at det skal lagres informasjon om hvor de ulike cellene befinner seg så lenge det lagres informasjon om kommunikasjonsdata. Tilbyderne må lagre en oversikt over hvilke geografiske områder som dekkes av hver enkelt celle.

3.2.1.7 Data som angir innholdet i kommunikasjonen

I art. 5 nr. 2 presiseres det at innholdet i kommunikasjonen ikke kan lagres med hjemmel i direktivet. Hva som blir sagt i samtalene eller skrevet i sms'er osv. vil altså ikke være gjenstand for lagring etter datalagringsdirektivet.

3.2.2 Norsk rett

3.2.2.1 Data som sporer og identifiserer kilden til en kommunikasjon

Når det gjelder det telefonnummeret som brukeren er tildelt (A-nummeret), må det først avklares om det er "trafikkdata", slik at ekomloven § 2-7, annet ledd kommer til anvendelse. Dette er opplysninger som tilsvarer datalagringdirektivet art. 5, 1. a) 1) i).

Brukerens telefonnummer er data som er nødvendig for å overføre kommunikasjon eller for fakturering av overføringen, jf. definisjonen i ekomforskriften § 7-1. A-nummer omfattes også av eksempelet i forarbeidene til ekomloven[39], da dette er data som "angir kommunikasjonens opphavssted". Når jeg konkluderer med at A-nummeret er "trafikkdata", innebærer det, slik jeg har vist ovenfor[40], at ekomloven § 2-7, annet ledd kommer til anvendelse, og både fysiske og juridiske personer omfattes.

Brukerens telefonnummer er data som er "nødvendig" for tilbyder å kunne lagre i henhold til faktureringsformålet. Opplysningene om kundens bruk må knyttes til abonnementet, for at tilbyder skal kunne fakturere kravet.

Brukerens telefonnummer (A-nummeret) kan altså lagres etter dagens regelverk.

Neste spørsmål er om opplysninger om abonnenten eller den registrerte brukeren, slik som navn og adresse (sml. art. 5, nr. 1. a) 1) ii)) er "trafikkdata".

---

[39] Ot.prp. nr. 58 (2002-2003) s. 92

[40] Jf. punkt 2.4.3

Det er mer uklart om ”trafikkdata” omfatter data som dette. Forskriftens definisjon sier at ”trafikkdata” er opplysningene som er nødvendige for fakturering. Navn og adresse på brukeren er opplysninger som er nødvendige for fakturering, men det menes ikke her mer teknisk data? Blant forarbeidenes eksempler finner vi ”kommunikasjonens opphavssted”. Det siktes trolig her til det telefonnummer som sender ut signaler, slik at brukerens navn og adresse ikke omfattes av ekomloven § 2-7. Det gjelder derimot en lagringsplikt for slike opplysninger etter ekomforskriften § 6-2, første ledd[41]:

> ”Tilbyder av offentlig telefontjeneste skal føre oversikt over enhver sluttbrukers navn, adresse og nummer/adresse for tjeneste”.

Denne lagringsplikten gjelder både overfor juridiske og fysiske brukere, jf. ekomloven § 1-5 nr. 12.

Det finnes altså en lagringsadgang i norsk lov idag når det gjelder opplysninger som faller inn under datalagringsdirektivet art. 5 nr. 1. a) 1) i), det vil si A-nummeret til brukeren. For brukerens navn og adresse, jf. art. 5 nr. 1 a) 1) ii) foreligger det allerede en lagringsplikt, jf. ekomforskriften § 6-2, første ledd.

3.2.2.2 Data som fastslår en kommunikasjons bestemmelsessted

Neste spørsmål blir om det også etter gjeldende rett i Norge lovlig kan lagres opplysninger om mottakeren av oppringningen, med andre ord B-nummeret, sml. Datalagringsdirektivet art. 5 nr. 1. b) 1) i).

[41] Jf. ekomloven § 2-8, tredje ledd

Dette er opplysninger som omfattes av ”trafikkdata” jf. ekomforskriften § 7-1 og forarbeidene til ekomloven[42] (”angir kommunikasjonens bestemmelsessted”), og dermed gjelder sletteplikten (og lagringsadgangen) etter ekomloven § 2-7, annet ledd. Opplysningene er ”nødvendig” for både kommunikasjons- og faktureringsformål. Dette kommer av brukerens rett til å få spesifisert telefonregningen sin. Denne skal kunne få en oversikt over hvem han har ringt, slik at eventuelle tvister kan unngås eller løses.

Etter datalagringsdirektivet skal også navn og adresse til abonnenten av B-nummeret lagres, jf. art. 5 nr. 1. b) 1) ii). Disse opplysningene regnes trolig ikke som ”trafikkdata”, jf. det jeg sa ovenfor under punkt 3.2.2.1. Med ”trafikkdata” menes nok opplysninger som er mer knyttet til selve kommunikasjonen[43]. Navn og adresse på en mottaker er imidlertid ”personopplysninger”, ettersom det kan ”knyttes til en enkelt person”, jf. personopplysningsloven § 2 nr. 1. Slike opplysninger skal slettes med mindre de er ”nødvendige”, jf. personopplysningsloven § 28. Det kan uansett ikke anses ”nødvendig” å lagre navn og adresse til abonnenten av B-nummeret hverken for et kommunikasjons- eller et faktureringsformål. Teletjenester kan overføres selv om tilbyder ikke har lagret opplysninger om mottakerens navn og adresse, og videre kan fakturering skje. Spesifisert faktura oppnås ved angivelse av det telefonnummer som er ringt, ikke nødvendig med ytterligere opplysninger om brukeren av dette nummeret.

Det foreligger altså en lagringsmulighet i norsk rett idag når det gjelder selve B-nummeret, men ikke når det gjelder navn og adresse til brukeren av dette nummeret.

3.2.2.3 Data som fastslår en kommunikasjons dato, klokkeslett og varighet

Opplysninger om dato, klokkeslett og varighet for telefonsamtalene eller sms-forsendelser mv. (sml. Datalagringsdirektivet art. 5, 1. c) 1)) er data som faller inn under ”trafikkdata”-

[42] Ot.prp. nr. 58 (2002-2003) s. 92

[43] Se Ot.prp. nr. 64 (1998-1999) s. 159 der trafikkdata ble definert som ”andre data knyttet til kommunikasjon”

begrepet, se forskriften § 7-1 og eksemplifiseringen i forarbeidene til ekomloven[44], og dermed gjelder ekomloven § 2-7, annet ledd.

Disse opplysningene er uten tvil nødvendige for å kunne spesifisere tilbyders krav. Det er nettopp varigheten for samtalene som avgjør fakturabeløpet. Videre må dato og klokkeslett for dataene anses ”nødvendig” for spesifikasjon av regningen.

Opplysninger om dato, klokkeslett og varighet for kommunikasjon via mobil- eller fasttelefon kan med andre ord lagres etter gjeldende norsk rett.

3.2.2.4 Data som identifiserer kommunikasjonstypen

Data som identifiserer hvilken kommunikasjonstype som har funnet sted, sml. datalagringsdirektivet art. 5 nr. 1. c) 1) og 5 nr. 1. d) 1), er også opplysninger som omfattes av definisjonen av ”trafikkdata”, og da gjelder sletteplikten og lagringsadgangen etter ekomloven § 2-7, annet ledd.

Det er nødvendig for tilbyder å kunne angi hva brukeren har benyttet telefonen til, da dette bestemmer fakturabeløpet. Hvorvidt brukeren har benyttet telefonen til samtaler eller forsendelse av sms eller mms er avgjørende for størrelsen på kravet, og derved er nødvendighetsvilkåret klart oppfylt.

Det er derfor også nå mulig å lagre opplysninger om kommunikasjonstype i Norge.

3.2.2.5 Data som identifiserer brukerens kommunikasjonsutstyr

Brukerens IMEI og IMSI-nummer skal lagres etter datalagringsdirektivet art. 5 nr. 1. e) 2) ii) og iii). For å avgjøre om disse opplysningene kan loggføres idag må de omfattes av ekomloven § 2-7, annet ledd eller personopplysningsloven § 28.

---

[44] Ot.prp. nr. 58 (2002-2003) s. 92

IMSI-nummeret omfattes av ”trafikkdata”-begrepet. Dette er data som er ”nødvendig for å overføre kommunikasjon”[45] og ”som angir kommunikasjonens (...) bestemmelsessted”[46]. IMSI-nummeret faller derfor inn under ekomloven § 2-7, annet ledd. Lagringen må imidlertid også være ”nødvendige” for å være lovlig. En brukers IMSI-nummer er nødvendig å loggføre for å kunne identifisere brukeren ved internasjonale samtaler, og videre kunne fakturere denne for slik bruk over landegrensene.

Når det gjelder IMEI-nummeret, stiller saken seg noe annerledes og mindre klar. Imei-nummeret er knyttet til den enkelte mobiltelefon og knytter denne til produsent, modelltype og hvilket land som har godkjent utstyret. Når man benytter telefonen til kommunikasjon, skjer det en registrering av IMEI-nummeret. Trolig er det tale om ”trafikkdata”, som omfattes av ekomloven § 2-7, annet ledd.

Lagringen må videre være ”nødvendig” for å være lovlig. Brukerens IMEI-nummer lagres idag i henhold til fakturaformålet, blant annet der en mobiltelefon er solgt med binding til en bestemt telefon. Lagrede IMEI-numre benyttes også til å sperre stjålne telefoner.

Når det gjelder B-abonnentens IMEI- og IMSI- nummer, er også dette ”trafikkdata” etter ekomloven § 2-7, annet ledd. Lagring av disse opplysningene er imidlertid på ingen måte nødvendig utover kortvarig lagring for kommunikasjonsformålet.

Etter gjeldende rett kan A-abonnentens IMSI- og IMEI-nummer lagres. Det kan ingen av disse numrene knyttet til B-abonnenten.

---

[45] Ekomforskriften § 7-1, første ledd, annet punktum.

[46] Ot.prp nr. 58 (2002-2003) s. 92

3.2.2.6 Data som foretar en lokalisering av mobilt utstyr

Etter datalagringsdirektivet art. 5, 1. f) 1) og 2) skal brukerens posisjonsdata lagres, det vil si opplysninger om celle-ID.

Dette er opplysninger også angitt som ”lokaliseringsdata”, og anses som noe annet enn ”trafikkdata”. Posisjonsdata som dette kan eventuelt være en annen form for ”personopplysning”. Dette er opplysninger som ”kan knyttes til en enkeltperson”, og dermed må personoppysningsloven gjelde. For å kunne oppbevares i henhold til personoppysningsloven § 28, må det være ”nødvendig” for tilbyder å lagre disse opplysningene for fakturering eller kommunikasjonsoverføring.

Data som angir hvor brukeren har befunnet seg mens telefonabonnementet hans har vært i bruk, er ikke nødvendig for faktureringsformålet.

Det er med andre ord ingen regler i norsk rett idag som tilsier at det skal lagres opplysninger som angir celle-ID.

3.2.2.7 Data som angir innholdet i kommunikasjonen

Data som angir innholdet i kommunikasjonen er ikke å anse som ”trafikkdata” som kan lagres etter ekomloven § 2-7, annet ledd, da det ikke er ”nødvendig” for tilbyder å lagre innholdet av brukerens telefonsamtaler eller meldinger for å kunne fakturere ham.

Tilbyder må kunne lagre innholdet i en sms frem til denne er kommet frem til mottaker, men dette er imidlertid ikke en langvarig form for lagring som vil være av betydning.

Opplysninger om kommunikasjonens innhold skal slettes etter norsk rett.

3.3 Internettadgang, e-mail og telefoni via internett

3.3.1 Datalagringsdirektivet

3.3.1.1 Data som sporer og identifiserer kilden til en kommunikasjon

Som ved telefonitjenester, skal det også for kommunikasjon via internett lagres opplysninger som identifiserer og sporer kilden, jf. art. 5 nr. 1 a) 2).

Ved internettbruk og e-mail og telefoni via internett skal brukeridentiteten registreres og lagres. Dette følger av i). I følge art. 2, 2. d) defineres brukeridentitet som ”en entydig identifikator, der tildeles en person, når vedkommende tegner abonnement...”. Det henvises her til brukerens sambandsnummer.

Nr ii) gjelder opplysninger om brukerkilden ved bruk av IP-telefoni. Brukeridentiteten og telefonnummeret skal da lagres av tilbyder. Brukerens telefonnummer ved IP-telefoni er ikke stedstilknyttet, som ved fasttelefoni. Uansett hvor bruker logger seg på sitt IP-telefoniabonnement, benyttes dette telefonnummeret. Sambandsnummer og IP-adresse skal lagres parallelt ved bruk av IP-telefoni.

Til sist skal brukerens/abonnentens navn og adresse loggføres.

3.3.1.2 Data som fastslår en kommunikasjons bestemmelsessted

For å kunne angi bestemmelsesstedet for kommunikasjonen, skal det loggføres opplysninger som gjelder mottakeren av e-mail eller telefoni via internett som kommer fra abonnenten. Det gjelder både mottakers brukeridentitet eller telefonnummer og dennes navn og adresse, jf. art. 5 nr. 1 b) 2) i) og ii).

3.3.1.3 Data som fastslår en kommunikasjons dato, klokkeslett og varighet

Videre skal dato, klokkeslett og varighet lagres, som for fast- og mobiltelefoni, jf. art. 5 nr. 1 c) 2) i).

For internettadgang innebærer dette lagring av tidspunkter for inn- og utlogging på internettjeneste. Det må også registreres hvilken tidssone brukeren befinner seg i for å anslå klokkeslettet presist. Uten å knytte oppkoblingen til en bestemt tidssone, er informasjonen naturlig nok verdiløs.

Den dynamiske eller statiske IP-adressen skal herunder loggføres av tilbyder. Vanlige brukere har som regel Dynamisk IP-adresse. Dette fungerer slik at IP-adresser lånes ut ved brukerens pålogging, slik at ulike brukere kan ha samme IP-adresse, men til ulik tid. Grunnen til dette er at det ikke finnes nok IP-adresser til at alle brukere kan ha hver sin faste. Den dynamiske IP-adressen en bruker får tildelt, låses ofte, slik at brukeren beholder den samme IP-adressen for en liten tidsperiode. Statisk IP-adresse er nødvendig for de som tilbyr tjenester og informasjon over nettet, som for eksempel en nettavis. Brukeren får da beholde samme IP-adresse gjennom hele sin abonnementsperiode.

For e-mailtjeneste og telefonitjeneste over internett skal samme type tidspunktinformasjon for inn- og utlogging lagres jf. ii).

3.3.1.4 Data som identifiserer kommunikasjonstypen

For e-mail og telefoni via internett skal det lagres opplysninger om kommunikasjonstypen, direktivet angir det som ”den anvendte internettjeneste”, jf. art 5 nr. 1 d) 2). Dette betyr at tilbyder skal registrere i sin logg om det eventuelt er e-mail eller telefoni som er benyttet ved internettilgangen.

3.3.1.5 Data som identifiserer brukerens kommunikasjonsutstyr

Etter art. 5 nr. 1 e) skal tilbyder foreta lagring av data for å identifisere brukerens kommunikasjonsutstyr. Det vil si A-nummeret og abonnentlinjen jf. art. 5 nr. 1 e) 3) i) og ii).

Ved bruk av modem som oppkobling til internett, der du bruker en vanlig telefonlinje for å få internettadgang, skal denne telefonlinjens A-nummer lagres. Ved oppkobling via digital abonnentlinje (DSL) eller noe annet enn DSL, eks ICE/trådløst bredbånd, skal dette lagres.

3.3.1.6 Data som angir innholdet i kommunikasjonen

Også for kommunikasjon via internett gjelder art. 5 nr. 2, som bestemmer at innholdet i kommunikasjonen ikke skal lagres.

3.3.2 Norsk rett

3.3.2.1 Data som sporer og identifiserer kilden til en kommunikasjon

Spørsmålet først er om brukeridentitet, telefonnummer og IP-adresser (sml. Datalagringsdirektivet art. 5 nr. 1. a) 2) i), ii) og iii)) er "trafikkdata" som omfattes av ekomloven § 2-7, annet ledd.

Brukeridentiteten og telefonnummeret er nødvendig for fakturering av et internettabonnement, jf. forskriftens definisjon[47]. En IP-adresse er data som angir kommunikasjonens opphavssted, jf. eksemplifiseringen i forarbeidene[48]. Det er fra brukerens tildelte IP-adresse informasjonen sendes ut.

Brukeridentiteten (sambandsnummer) og telefonnummer ved telefoni via internett er opplysninger som må anses "nødvendige", da de brukes for å sende ut faktura, enten det gjelder bredbåndsabonnementer eller dial-up. Fakturering må kunne kobles til et abonnementsnummer. Det er mer uklart om en tildelt IP-adresse er å anse som "nødvendig" for et av de nevnte formål. Idag godtas lagring av IP-adresser for en begrenset tidsperiode,

[47] Ekomforskriften § 7-1, første ledd, annet punktum

[48] Ot.prp. nr. 58 (2002-2003) s. 92

se brev fra datatilsynet til IKT-Norge[49], der det settes en frist til lagring i tre uker (mer om denne tidsfristen i kapittel 6).

Dermed er både brukeridentitet, telefonnummer ved telefoni via internett og tildelte IP-adresser opplysninger som lagres med hjemmel i norsk rett idag.

3.3.2.2 Data som fastslår en kommunikasjons bestemmelsessted

Etter datalagringsdirektivet skal det videre lagres opplysninger om mottakeren av e-post eller telefonoppkall via internett, se art. 5 nr. 1. b) 2) i) og ii).

Brukeridentitet eller telefonnummer til mottakeren faller nok inn under ”trafikkdata” etter ekomloven § 2-7, annet ledd, jf. eksemplene i forarbeidene til loven[50] som blant annet nevner data som ”angir kommunikasjonens opphavssted”.

Telefoni via internett er også kjent som ”IP-telefoni”, og er telefonsamtaler hvor signalene blir fraktet over internett. Det finnes to typer IP-telefoni. Den ene minner om et vanlig telefonabonnement, hvor abonnenten mottar faktura etter bruk. Den andre er en gratis tjeneste uten noen form for samtaleregistrering. Abonnenten av telefoni som dette mottar ikke en egen regning for telefonsamtalene han foretar via internett, men belastes via internettbruken, avhengig av hvilken type internettabonnement han har. Hvor brukeren har et bredbåndsabonnement, vil ikke det faste månedlige beløpet endres etter antall IP-telefonsamtaler. Ved modemsbasert internett avgjøres fakturabeløpet etter antall tellerskritt internett er tilkoblet, uansett hva brukeren benytter internettilgangen til. Når det gjelder betalingspliktig IP-telefoni, må det regnes som ”nødvendig” å lagre mottakerens telefonnummer, for å kunne gi bruker spesifisert regning. For øvrig er dette opplysninger som ikke kan anses ”nødvendige” for faktureringsformål. Opplysninger om mottakerens brukeridentitet må imidlertig kunne lagres for at tilbyder skal kunne gjennomføre tjenesten,

[49] Datatilsynet 13. mai 2009 s. 2

[50] Ot.prp. nr. 58 (2002-2003) s. 92

med andre ord overføre telefonsamtalen eller e-posten. Dette er lagring i henhold til kommunikasjonsformål, men vil være så kortvarig at jeg ikke tar det i betraktning her.

Navn og adresse på mottaker vil imidlertid ikke i noe tilfelle kunne anses å være "nødvendige" opplysninger etter ekomloven § 2-7, annet ledd.

Kort oppsummert er det kun hjemmel for lagring av mottakers telefonnummer ved betalingspliktig IP-telefoni i Norge i dag. Øvrige opplysninger om bestemmelsessted etter datalagringsdirektivet art. 5 nr. 1. b) 2) i) og ii skal slettes.

3.3.2.3 Data som fastslår kommunikasjonens dato, klokkeslett og varighet

Data som fastslår dato, klokkeslett og varighet for kommunikasjonen inngår i definisjonen av "trafikkdata", jf. forarbeidene til ekomloven[51].

For å angi hva som er "nødvendig" for tilbyder å lagre, etter ekomloven § 2-7 annet ledd, må vi skille mellom modemsbasert internett og bredbånd. Der kunden har et modemsbasert internett, avgjøres tilbyderns fakturakrav av faktisk bruk. Derfor har tilbyderen behov for å lagre data som angir når brukeren er tilkoblet internett, og hvor lenge denne bruken varer. Dette er opplysninger som tilsvarer datalagringsdirektivet art. 5 nr. 1. c) 2) i) og ii). Bredbåndsabonnementer faktureres med et fast månedlig beløp, uavhengig av faktisk bruk. I slike tilfeller vil det ikke være "nødvendig" for tilbyder å kunne lagre opplysninger om når kunden er tilkoblet internett.

Hva med internett via mobiltelefon og mobilt bredbånd? Dette er internettilgang hvor det foreligger ulike faktureringsformer. Det finnes abonnementer som kan sidestilles med bredbånd, hvor bruken ikke har betydning for fakturabeløpe, og det finnes abonnementer hvor antall nedlastingsenheter har betydning, dvs hvor stor datamengde som lastes ned av brukeren. For sistnevnte internettingangstype må tilbyder ha anledning til å lagre bruken

[51] Ot.prp. nr. 58 (2002-2003) s. 92

etter ”nødvendighetskriteriet”. Men er tidspunktene for bruken ”nødvendig”? Trolig må det være det, for å kunne vise til når nedlastingen har foregått. På samme måte som ved vanlig telefoni og modemsbasert internett, kan det oppstå tvist rundt fakturabeløpet, slik at tilbyder må kunne ha spesifike data å vise til for å løse denne.

Ved bruk av betalingspliktig IP-telefoni, må tidspunkt for inn- og utlogging kunne lagres av hensyn til fakturaformålet også idag. På samme måte som ved den gratis formen for IP-telefoni skjer det ingen egen fakturering av e-post. For e-post- og øvrig IP-telefoni kan derfor ikke tilsvarende gjelde, ettersom inn- og utlogging ikke har betydning for fakturabeløpet.

Idag kan med andre ord tilbyder lagre opplysninger om dato, klokkeslett og varighet knyttet til modemsbasert internett og mobile bredbånd hvor faktisk bruk er avgjørende for fakturabeløp. De kan også lagre tilsvarende data for betalingspliktig IP-telefoni. Ved bredbåndsabonnementer og mobile bredbånd med ”fri bruk”, skal opplysningene slettes straks. Det samme gjelder for inn- og utlogging fra e-post eller gratis IP-telefoni.

3.3.2.4 Data som identifiserer kommunikasjonstypen

Neste spørsmål er hvorvidt data som angir hvorvidt brukeren har benyttet internett til IP-telefoni eller e-post, sml. datalagringsdirektivet art. 5 nr 1. d) 2), er ”trafikkdata” som reguleres av ekomloven § 2-7, annet ledd. Utover betalingspliktig IP-telefoni, er dette opplysninger som ikke omfattes av definisjonen i ekomforskriften § 7-1, og kan dermed ikke lagres i henhold til ekomloven.

Det må da spørres om dette er ”personopplysninger” etter personopplysningsloven. Kan slike data ”knyttes til en enkeltperson”? Kan nok konkludere med det. Uansett er det ikke ”nødvendig” for tilbyder å lagre hvorvidt brukeren har vært tilkoblet e-post eller IP-telefoni, utover det som lagres om bruken av dette, jf. ovenfor.

Per idag kan det altså lagres at brukeren har vært koblet til IP-telefoni, der bruk av dette medfører betalingsplikt. Ellers foreligger det ingen adgang til lagring av data som angir at bruker har benyttet internett til e-postforsendelse eller annen form for IP-telefoni.

3.3.2.5 Data som identifiserer brukerens kommunikasjonsutstyr

A-nummeret til brukeren ved dial-up adgang til internett (sml. Datalagringsdirektivet art. 5 nr 1. e) 3) i)) er å anse som "trafikkdata", jf. ekomforskriften § 7-1. Opplysningene må kunne lagres idag, i henhold til faktureringsformål. Dette har sammenheng med at utskrivelse av faktura må knyttes til en abonnementsangivelse, hvilket A-nummeret er. Det samme gjelder opplysninger om brukerens abonnentlinje ved bredbåndsabonnement, sml. Datalagringsdirektivet art. 5 nr. 1 e) 3) ii).

Disse data kan med andre ord lagres idag.

3.3.2.6 Data som angir innholdet i kommunikasjonen

Data som angir innholdet i brukerens internettbruk er ikke "trafikkdata", da det ikke er "nødvendig" jf. ekomforskriften§ 7-1. Dermed gjelder ikke ekomloven § 2-7, annet ledd for opplysninger knyttet til dette.

Slike data kan defineres som "personopplysninger" etter personopplysningsloven[52], men ettersom lagring av innholdet i e-post eller telefoni over internett ikke er "nødvendig" for fakturering, skal de slettes, jf. personopplysningsloven § 28.

Også her gjelder imidlertid en veldig kortvarig lagringsadgang i henhold til kommunikasjonsformålet, ved oversendelse av e-post. Innholdet av denne må lagres frem til den er kommet frem til mottakers innboks.

---

[52] Kan "knyttes til enkelt person", jf. personopplysningsloven § 2 nr. 1

3.4 Endring/sammenligning

3.4.1 Innledning

Her vil jeg, som nevnt i punkt 1.1, angi hvilke endringer det er tilstrekkelig å foreta i norsk lovverk for å gjennomføre innholdet i lagringsplikten etter datalagringsdirektivet. Hvilken måte det vil være mest hensiktsmessig å gjøre dette på, vil jeg først konkludere med etter å ha funnet ut hvor store endringer det totalt sett kreves for å oppfylle direktivet. Denne drøftelsen vil jeg foreta i kapittel 8 i avhandlingen.

3.4.2 Telefoni

Når det gjelder fasttelefoni og mobiltelefoni, har vi sett at de største endringene ved innføring av datalagringsdirektivet vil være lagring av posisjonsdata ved mobilbruk. Ved at det kommer en lagringsplikt for celle-ID vil påtalemyndighetene kunne kreve utlevert tilbyderes logger for å fastslå hvor den bestemte bruker befant seg på ulike tidspunkter mens mobiltelefonen har vært i bruk. For å oppfylle datalagringsdirektivets krav må Norge dermed vedta lovbestemmelser som gir tilbyder av fasttelefoni og mobiltelefoni en plikt til å lagre opplysninger om hvilke basestasjoner bruker har vært oppkoblet mot mens telefonen har vært i bruk.

Jeg konkluderte i punkt 3.2.2.6 med at lokaliseringsdata som dette ikke er ”trafikkdata”, men omfattes av definisjonen av ”personopplysninger”[53], slik at det må skje en endring av personoppysningsloven. En ny bestemmelse kan plasseres i ekomloven ettersom denne går foran personoppysningsloven ved motstrid[54]. Dette vil være mest hensiktsmessig, og gir en mer riktig plassering i lovverket for å få samsvar med de andre reglene datalagringsdirektivet innebærer.

[53] Jf. Personoppysningsloven § 2 nr. 1).

[54] Jf. Punkt 2.4.3

Vi har også sett at innføring av lagring av navn og adresse på mottaker av telefonsamtaler, sms osv innebærer en viss endring i forhold til dagens lovverk. Som nevnt er dette ”personopplysninger”, slik at personopplysningsloven må endres. Som ovenfor kan også disse endringene gjennomføres i ekomloven, noe de også bør. Bestemmelsen må konkretisere innholdet i lagringsplikten, slik at også disse opplysningene omfattes.

Under punkt 3.2.2.5 konkluderte jeg med at datalagringsdirektivet vil innebære en endring når det gjelder lagring av mottakeres IMSI- og IMEI-numre. Dette er trafikkdata, og en bestemmelse som angir at dette skal lagres, må plasseres i ekomloven.

3.4.3 Internettadgang, e-mail og telefoni via internett

For internettjenester vil det skje mer omfattende endringer dersom datalagringsdirektivet implementeres i norsk rett.

For det første må tilbyder nå lagre brukeridentiteten til mottaker av e-post eller IP-telefoni og hvilken tjeneste brukeren har benyttet internett til[55], videre innføres opplysninger om kommunikasjonstype som lagringsobjekter[56], og også tidspunktene for inn- og utlogging av e-post og telefoni skal lagres etter datalagringsdirektivet. Videre innføres lagring av opplysninger som angir når brukeren har logget seg av og på internett der brukeren er en bredbåndsabonnent[57].

Alle disse opplysningene er å anse som ”trafikkdata”. Derfor må ekomloven få en bestemmelse som innebærer at brukeridentiteten til mottaker av e-post og IP-telefonsamtaler, opplysninger om kommunikasjonstype, tidspunkt for inn- og utloggen av e-post og IP-telefoni skal lagres.

---

[55] Se punkt 3.3.2.2 ovenfor

[56] Se punkt 3.3.2.4 ovenfor

[57] Se punkt 3.3.2.3 ovenfor

4 En overgang fra sletteplikt til lagringsplikt

4.1 Datalagringsdirektivet

Dersom EU-direktivets innhold gjennomføres som en del av norsk rett, opprettes en plikt til lagring av opplysninger angitt i direktivets art. 5 for aktører innenfor tele- og internettbransjen. Denne forpliktelsen følger direkte av direktivets artikkel 3 nr. 1: "Obligation to retain data". Medlemslandene skal sikre at "data" lagres etter direktivet. Hvilke data dette er har jeg redegjort for i kapittel 3 i avhandlingen.

Direktivet etterlater ingen mulighet til fravikelse fra den oppstilte lagringsplikt. Tilbyder har dermed ingen valgfrihet med hensyn til lagring av trafikkdata, men er ubetinget forpliktet til å ha direktivets nærmere angitte opplysninger (jf. art. 5, se kapittel 3) lagret i den perioden direktivet/gjennomføringsloven fastsetter (jf. art. 6, se kapittel 6 nedenfor).

4.2 Norsk rett

Som utgangspunktet i norsk rett idag gjelder en sletteplikt for opplysninger av personlig art. Denne plikten følger av ekomloven § 2-7, annet ledd og personopplysningsloven § 28. Idag har tilbydere av elektronisk kommunikasjonstjeneste ingen plikt til noen form for lagring av trafikkdata, men kan lagre slike opplysninger dersom lagringen er "nødvendig" for kommunikasjons- eller faktureringsformål. Det foreligger med andre ord en lagringsadgang for disse opplysningene.

Bestemmelsene må sees i sammenheng med personopplysningsloven § 33 og personopplysningsforskriften[58] § 7-1, som regulerer konsesjonsplikt for behandling av personopplysninger. Forskriftens § 7-1 innebærer at enhver tilbyder av teletjenester må

[58] Jf. personopplysningsloven § 33, annet ledd

søke konsesjon for å kunne operere i bransjen. Det må derfor også antas at bransjepraksis vil være å lagre opplysninger om brukernes trafikkdata i henhold til den gitte konsesjon. Dette er en naturlig følge av muligheten til å fravike sletteplikten, ettersom en må anta at tilbyderne selv ønsker og anser det nødvendig å oppbevare opplysninger slik konsesjonen gir adgang til. En kan da si at utgangspunktet etter dette naturlig nok blir lagring av "nødvendige" opplysninger om brukernes trafikkdata i en bestemt periode, istedet for umiddelbar sletting slik loven angir.

4.3 Sammenligning/endringer

Innføring av datalagringsdirektivet i norsk rett vil innebære at tilbyderne i tele- og internettbransjen får et lagringssystem for opplysninger, redegjort for under kapittel 3 i avhandlingen, uavhengig av egne behov og av kundenes ønsker. Der det nå gjelder en sletteplikt som utgangspunkt, jf. ekomloven § 2-7, annet ledd og personopplysningsloven § 28, vil det som en sterk kontrast innføres en ubetinget lagringsplikt, jf. datalagringsdirektivet art. 3 nr. 1. Ut fra dette må det spørres hvilke legislative grep som må til for å gjennomføre denne lagringsplikten i norsk rett.

Ekomloven går foran personopplysningsloven (jf. punkt 2.4.3 ovenfor). Det innebærer at først og fremst må ekomloven endres. Men det må også skje en endring i personopplysningsloven. Som sett i kapittel 3, punkt 3.4 innebærer datalagringsdirektivet art. 5 at enkelte "personopplysninger", jf. personopplysningsloven § 2 nr. 1, som ikke samtidig er "trafikkdata" etter ekomloven, omfattes av lagringsplikten i datalagringsdirektivet art. 4. Det kan ikke lenger i norsk rett foreligge en plikt til sletting av de angitte personopplysningene, og lagring må skje uten en nærmere nødvendighetsprøving. I stedet må det komme en ubetinget lagringsplikt som hovedregel for den type trafikkdata og andre personopplysninger direktivet angir lagringsplikt for. Etter at datalagringsdirektivets minimumskrav til lagringstid er utgått, kan og bør imidlertid begge lovene kreve sletting av de lagrede data.

5 Lagringens formål – Hva skal opplysningene brukes til?

5.1 Datalagringsdirektivet

Datalagringsdirektivets artikkel 1 angir formålet for innføring av lagringsplikt:

> "...in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law"

Formålet skal etter direktivet være bekjempelse av grov kriminalitet, men det er opp til det enkelte medlemsland å definere nærmere hva som skal anses som "grov kriminalitet". Stikkordene for formålet er "investigation, detection and prosecution", eller "etterforskning, avsløring og rettsforfølgelse" oversatt til norsk[59].

Når det gjelder de straffeprosessuelle grepene etterforskning ("investigation") og rettsforfølgning ("prosecution"), foregår de på et tidspunkt i politiets arbeidet hvor det foreligger en bestemt mistenkt, siktet (strpl. § 82) eller tiltalt (se Hov II s. 201 og s. 83). På etterforskningsstadiet ("investigation") har det skjedd et lovbrudd, og påtalemyndigheten har i denne sak én eller flere mistenkte eller siktede å forholde seg til. På bakgrunn av dette oppsøkes opplysninger som knytter seg til dennes eller disses aktivitet via elektronisk kommunikasjon. I forbindelse med at en person får stilling som mistenkt eller siktet i en sak, får denne en rekke rettigheter som skal ivareta hans stilling. Blant annet kan nevnes retten til å begjære rettergangsskritt for å avkrefte mistanken (strpl. § 241) og retten til innsyn i sakens dokumenter (strpl. § 242). På rettsforfølgningsstadiet ("prosecution") er tiltaltes stilling ennå klarere. Her har påtalemyndigheten valgt å gå til sak mot en de anser som sannsynlig lovbryter i saken de står overfor (se strpl. § 252 og Hov s. 83), og må

[59] Kunnskapsforlagets Engelsk blå ordbok

kunne få tilgang til opplysninger vedrørende dennes kommunikasjon via telefon og internett. Det foreligger her en konkretisering av hvem opplysningene knytter seg til.

Direktivet åpner imidlertid i tillegg for at de lagrede opplysninger skal kunne brukes til "detection of (...) serious crime", jf. art. 1 nr. 1 i.f. For å kunne ta standpunkt til innholdet i dette, må en ta utgangspunkt i en naturlig språklig forståelse av ordlyden. Oversatt til norsk vil "detection" innebære "avsløring, oppdagelse, oppsporing, påvisning, oppklaring..." (ordboka). Én forståelse kan etter dette være at det skjer en avklaring av at en bestemt forbrytelse har funnet sted, på et etterforskningsstadie. Det "påvises" at noe kriminelt har skjedd, noe som påtalemyndighetene allerede har mistanke om. Bestemmelsen kan imidlertid også leses som at politiet allerede på et tidligere tidspunkt skal ha tilgang til opplysningene, allerede før det er oppdaget et lovbrudd som tilgangskravet kan knyttes til. Dette vil kunne innebære at påtalemyndighetene har en generell tilgang til å se over logger mv. for å se etter mistenkelig aktivitet.

De siste årene har det skjedd en stadig større kriminalisering av handlinger som foregår på et forberedelsesstadium, se blant annet straffeloven §§ 147a og 201a. Allerede planlegging av enkelte forbrytelser av mer alvorlig art kan i seg selv være straffbart etter disse bestemmelsene. Det er straffbart å planlegge, og forberedelsene skjer ofte ved kommunikasjon via telefon eller internett. Datalagringsdirektivet vil innebære at det blir lettere å avdekke slike kriminelle handlinger ved en form for "overvåking" av tilbydernes logger. Eksempelvis "grooming"-bestemmelsen i straffeloven § 201a som innebærer at det er straffbart å avtale møte med barn under 16 år med den hensikt å begå seksuelle forbrytelser overfor denne. Slike forsøk er kanskje ikke "grov kriminalitet", slik datalagringsdirektivet krever. Imidlertid må straffeloven § 147a, tredje ledd utvilsomt rammes av kriminalitetsbekjempelse etter datalagringsdirektivet. Bestemmelsen gjør det straffbart å planlegge eller forberede en terrorhandling ved å "inngå forbund med noen".

I denne forbindelse vil "detection"-funksjonen i datalagringsdirektivet art. 1 ha betydning. Dersom påtalemyndighetene gis tilgang til å få utlevert logger uten å knytte disse til en

konkret mistenkt, kan forberedelseshandlinger som dette avdekkes, noe som ellers ville vært vanskelig, ettersom kontakten (via telefon eller internett) skjer på et tidlig stadie, når det foreligger få signaler om lovbrudd. Her kan det tenkes at en tolking i retning av ”avklaring” vil være til hjelp for kriminalitetsbekjempelse. En slik bruk av ”detection” innebærer at lagret informasjon om hvem som har vært i kontakt med hverandre og når dette har skjedd kan avdekke at planlegging av for eksempel terrorvirksomhet har pågått, der en har fått tips eller mistanke om dette på annen måte. Større deler av ”forbundet” som har tatt del i planleggingen kan spores opp på denne måten.

Det er lite trolig at datalagringsdirektivet innebærer at påtalemyndighetene skal ha en såvidt vid innsynsadgang i tilbydernes logger. Det bør imidlertid være oppmerksomhet viet til muligheten for at EF-domstolen vil godta en slik tolking, også med virkning for Norge som EØS-land.

5.2 Norsk rett

5.2.1 Ekomloven og Personopplysningsloven

Dagens formål for lagring av trafikkdata er fakturering og kommunikasjonsbehandling. Dette følger direkte av ekomloven § 2-7, annet ledd.

Mange abonnenter ønsker å få spesifisert sine fakturaer i forhold til samtalemottakere og samtaletid, blant annet for å få oversikt over eget bruk. Behovet kan også komme som følge av tvist om fakturabeløpet, hvor tilbyderen har behov for å bevise den faktiske bruk for å begrunne sitt krav.

Kommunikasjonsformålet innebærer at visse opplysninger må oppbevares for å gjennomføre tjenesten. For eksempel ved forsendelse av en sms, lagres innholdet i denne til den er kommet frem til mottaker.

Personopplysningsloven § 28 sier ikke like klart hva formålet for lagringen skal være, men viser til ”formålet med behandlingen”. En utdyping av dette følger imidlertid av ”konsesjon til å behandle personopplysninger” for teletjenester punkt 1. Også etter personopplysningsloven skal lagring av opplysninger om bruk av tele- og internettjenester skje i kommunikasjons- eller fakturaøyemed.

5.2.2 Straffeprosesslovgivning

Til tross for at opplysninger om datatrafikk ifølge personopplysningsloven § 28 og ekomloven § 2-7, annet ledd skal lagres med det formål å overføre kommunikasjon, samt å spesifisere brukerens fakturabeløp (se ovenfor, punkt 4.2.1), brukes de lagrede dataene i stor grad til andre formål med lovhjemmel blant annet i straffeprosessloven. Dette har vært en ikke særlig omtvistet bruk av personopplysninger som allerede har ligget loggført hos tilbyderne av tele- og internettjenester.

Etter straffeprosessloven § 215a kan påtalemyndighetene kreve ”sikring av elektronisk lagrede data som antas å ha betydning som bevis”. Dette gjelder altså overfor data som allerede er lagret hos tilbyder i henhold til ekomloven § 2-7, annet ledd og personopplysningsloven § 28, og vil også tjene til hjemmel for opplysninger som eventuelt skal lagres etter datalagringsdirektivet. Sikring kan bare pålegges overfor tilbyder ”som ledd i etterforskning”, jf. første ledd, dersom det er ”grunn til å tro at det er begått en straffbar handling”, jf. annet ledd. Med andre ord må det foreligge en mistenkt som dataene kan knyttes til, enten ved at de direkte gjelder denne mistenkte, eller kan bidra til å spore denne opp. Den mistenkte skal etter bestemmelsens tredje ledd underrettes om sikringspålegget, og får stilling som siktet i saken når dataene er sikret.

Straffeprosessloven § 216 b, annet ledd bokstav d) gir påtalemyndigheten hjemmel til å kreve innsyn i mistenktes bruk av telefoni eller internett, uten at denne blir varslet om det. Etter denne bestemmelsens kan politiet få utlevert ”andre data knyttet til kommunikasjon”.

Dette må omfatte alle typer trafikkdata som omfattes av datalagringsdirektivet[60]. I tillegg gis det her hjemmel for utlevering av såkalte ”posisjonsdata”, det vil si opplysninger om celle-ID, som skal lagres etter datalagringsdirektivet art. 5 nr. 1 f) 1)[61] Dette er opplysninger som ikke skal lagres idag, jf. punkt 3.2.1.6 ovenfor. Hva innebærer da denne utleveringshjemmelen? Bestemmelsen gir adgang til utlevering av både historiske, lagrede data og i tilknytning til fremtidig kommunikasjon. Når det gjelder bruk av kommunikasjonsanlegg, må det være den fremtidige bruk regelen tar sikte på. Straffeprosessloven § 216 b setter vilkår for utlevering av trafikkdata. Det må foreligge skjellig grunn til mistanke, og handlingen (eller forsøket) må kunne medføre en fengelsstraff på minimum fem år, eller rammes av særskilt nevnte bestemmelser i straffeloven.

Videre regulerer straffeprosessloven § 210 utleveringspålegg. Også denne bestemmelsen er blitt brukt for å få utlevert tele- og internettilbyders logger. Her hjemles en omfattende utlevering av telefon- og internettrafikktrafikk. Etter bestemmelsen stilles det ikke krav om en viss strafferamme, slik som § 216 b gjør, men derimot kreves det rettslig kjennelse. Etter strpl. § 210 kan politiet kreve å få utlevert opplysninger om hvilke mobiltelefoner som har vært i forbindelse med en bestemt basestasjon i et bestemt tidspunkt (NOU s. 209). Disse opplysningene er det imidlertid ikke lovlig å lagre per idag. Derfor må bestemmelsen nå ta sikte på fremtidige data, slik som straffeprosessloven § 216 b gjør. For utlevering av fremtidige data etter § 210 gjelder imidlertid § 210b, som setter vilkår. Det må foreligge skjellig grunn til mistanke, og mulighet for straff i form av fengsel i minimum 5 år, eventuelt må handlingen rammes av bestemte regler i straffeloven. Ved implementering av datalagringsdirektivet vil § 210 kunne innebære utlevering av allerede lagret informasjon knyttet til basestasjontrafikk.

Alle disse bestemmelsene krever at den bruker hvis opplysninger det kreves innsyn i, har fått stilling som mistenkt i en sak. Dette innebærer at påtalemyndighetene per i dag har

[60] Se NOU 2009:15 s. 216

[61] Ot prp nr 64 (1998-99) s. 159

tilgang til registre over brukernes kommunikasjon på etterforsknings- og straffeforfølgningsstadiet, men ikke på et tidligere tidspunkt. I tillegg gjelder forholdsmessighetsprinsippet i straffeprosessloven § 170a både overfor § 215a, § 216 b og § 210. Dette vilkåret innebærer at et tvangsmiddel ikke kan benyttes dersom det vil være "et uforholdsmessig inngrep"[62]. Dette må avgjøres konkret.

Ekomloven § 2-9 gir politiet hjemmel til å få utlevert trafikkdata, ved at post- og teletilsynet opphever tilbyders taushetsplikt. Også etter denne utleveringshjemmelen er det krav om "skjellig grunn til mistanke om et konkret straffbart forhold", slik at det heller ikke her er tale om innsyn på et tidligere tidspunkt enn etterforskningsstadiet.

Politiloven § 17 d gir Politiets Sikkerhetstjeneste adgang til innsyn ved visse forberedelseshandlinger (blant annet straffeloven §§ 147a, 90, 91, 91a) etter rettskjennelse, under vilkår av at opplysningene kan forebygge de fremtidige handlinger som forberedes eller at forebyggingen "ellers i vesentlig grad vil bli vanskeliggjort". Det må foreligge "grunn til å undersøke om noen forbereder en handling" som faller inn under visse bestemmelser i straffeloven. I tillegg gjelder også her et forholdsmessighetskrav. Heller ikke her er det altså tale om å gi politiet et generelt innsyn i tilbyders logger.

Ut over dette er det ingen bestemmelser i nåværende prosesslovgivning som gir påtalemyndighetene innsyn i tilbydernes registre, og det er dermed ingen hjemler for innsyn på et tidligere tidspunkt enn der det faktisk finnes en mistenkt. Det er ingen regler som gir mulighet til generell overvåkning av registre som er ment til bruk som fakturagrunnlag.

[62] Se NOU 2009:15 s. 216

5.3 Endring/sammenligning

Fra å oppbevare trafikkdata som spesifiseringsgrunnlag for brukernes fakturaer, blir formålet ved innføring av datalagringsdirektivet kriminalitetsbekjempelse. Dermed blir det lovgitte formålet for lagring klart undergitt en endring.

Idag innebærer personopplysningsloven § 28 og ekomloven § 2-7, annet ledd at lagring kan skje for fakturerings- eller kommunikasjonsformål, men vi har sett at loggførte opplysninger likevel benyttes av påtalemyndighetene for å avdekke at det har skjedd kriminelle handlinger, der en har en mistenkt, siktet eller tiltalt i saken. Mye kan derfor tyde på at datalagringsdirektivets bestemmelser ikke vil innebære noen reell forskjell dersom de gjennomføres som norsk rett. Vil det da være nødvendig å endre norsk lov? Kan det sies å være tilstrekkelig med den ordlyd vi har idag, ettersom det likevel er mulig å utlevere opplysningene til påtalemyndighetene for å bekjempe kriminalitet?

Først må det spørres om vi må gjøre endringer i ekomloven og personopplysningsloven. Som jeg konkluderte med i punkt 4.3 må nødvendighetsvilkåret i henholdsvis § 2-7, annet ledd og § 28 utgå som begrunnelse for lagring av trafikkdata. Det er ikke dermed sagt at ekomloven og personopplysningsloven ikke lenger kan inneholde en bestemmelse lagring i kommunikasjons- eller fakturaformål. Etter at datalagringsdirektivets krav til lagringsplikt er utløpt[63], kan det holdes åpent for lagring i henhold til disse formål. Det aktuelle formålet vil da være fakturering, ettersom kommunikasjonsformålet utgår lenge før seks måneder[64] er gått. Det bør fortsatt være adgang til lagring etter dette formålet. Ikke alle tvister om fakturabeløp er nødvendigvis oppgjort når lagringsplikt etter datalagringsdirektivet ikke lenger foreligger. Derfor bør tilbyder ha en hjemmel som angir en adgang til videre lagring for nettopp fakturaformålet.

[63] Jf. datalagringsdirektivet art. 6, jf. kapittel 6 nedenfor.

[64] Jf. datalagringsdirektivet art. 6

Det er ikke strengt nødvendig å få lovfestet kriminalitetsbekjempelse som formål for lagring. Vi har sett at trafikkdata kan utleveres til påtalemyndighetene på tross av at ikke dette formålet følger av lov.

Det er videre et spørsmål om reglene i straffeprosessloven må endres. Når det gjelder utlevering av trafikkdata på et etterforsknings- eller rettsforfølgningsstadie, reguleres dette idag av straffeprosessloven §§ 215b, 216 b og 210. Problemstillingen blir om disse fremdeles kan benyttes som tilstrekkelig hjemmel for å oppfylle datalagringsdirektivet. Som vi så har straffeprosessloven § 215a en åpen ordlyd som omfatter "elektronisk lagrede data. Det samme gjelder § 216 b, som innebærer at påtalemyndighetene kan få utlevert "andre data knyttet til kommunikasjon". Dette må omfatte alle typer trafikkdata som skal lagres etter datalagringsdirektivet art. 5. Politiet kan også få utlevert "posisjonsdata", jf. datalagringsdirektivet art. 5 nr. 1 f) 1) etter de samme bestemmelser. Selv om det etter dagens rett kun kan være tale om fremtidige opplysninger knyttet til kommunikasjonsanlegg, åpner ordlyden for at også lagrede posisjonsdata kan utleveres. Dermed kreves ingen endring i straffeprosessloven §§ 215a og 216 b når det gjelder hvilke opplysninger som kan utleveres. Også straffeprosessloven § 210 har en ordlyd som åpner for bruk overfor alle opplysninger som skal lagres etter datalagringsdirektivet art. 5.

Datalagringsdirektivet gir ingen føringer om hvilke vilkår som kan stilles for utlevering av lagret informasjon om tele- og internettkunder. Når det kreves "skjellig grunn til mistanke" i norsk rett, jf. straffeprosessloven § 216 b, er det et krav som kan beholdes i norsk rett. Bestemmelsen angir videre spesifike lovbrudd hvor utlevering kan skje, eventuelt hvor strafferammen er minimum 5 år. Ettersom det etter datalagringsdirektivet er opp til medlemslandene å avklare hva som er "grov kriminalitet", kan også dette vilkåret bli stående.

Dersom en, med grunnlag i ordlyden "detection", legger til grunn at datalagringsdirektivet gir påtalemyndigheten en rett til å få utlevert opplysningsregistrene allerede før lovbrudd er oppdaget, eller til og med gjennomført, vil vi få en innsynshjemmel som ikke eksisterer

etter dagens lovgivning. Som vist ovenfor[65] finnes det ingen lovregler som idag gir påtalemyndighetene en slik innsynsrett. Direktivet vil da innebære en endring som må gjennomføres i norsk rett.

[65] Punkt 5.2.2

6 Omfang i tid – Hvor lenge skal opplysningene lagres?

6.1 Datalagringsdirektivet

Datalagringsdirektivet regulerer lagringstid i artikkel 6. Bestemmelsen gir medlemsstatene et valg mellom lagringstid på minimum 6 måneder og maksimalt 2 år.

Eventuelle EØS-rettslige forpliktelser kan oppfylles allerede ved 6 måneders lagringsplikt, og min avhandling vil dreie seg om en eventuell utvidelse til dette, jf. forutsetning i punkt 1.1.

6.2 Norsk rett

Opplysninger om brukernes trafikkdata skal slettes når de ikke lenger er ”nødvendige” for formålet med lagringen, se ekomloven § 2-7, annet ledd og personopplysningsloven § 28. For opplysninger som kan lagres etter norsk rett i dag avgjøres lagringstiden med andre ord etter et nødvendighetsprinsipp. Dette er en relativ frist hvor det vesentlige er hvor lenge det er ”nødvendig” for tilbyderen å oppbevare opplysningene. Denne redegjørelsen har kun betydning for opplysninger som tilbyder har adgang til å lagre i dag. Opplysninger som ikke kan loggføres lovlig (se kapittel 3) omfattes følgelig ikke av denne fremstillingen.

Hvor lenge en opplysning er ”nødvendig” vil variere etter hvert enkelt tilfelle og må avgjøres konkret. Der oppgjør har skjedd uten forbehold, er det klart at tilbyder ikke lenger har behov for å kunne dokumentere kundens bruk. Da skal opplysningene slettes umiddelbart. Dersom det har oppstått en tvist mellom tilbyder og bruker om fakturabeløpet på brukerens telefoni vil fristen bli tilsvarende lengre, slik at tilbyder kan oppbevare opplysningene om brukerens telefonbruk så lenge tvisten pågår. Ellers kan nødvendighetskriteriet være utløpt idet klagefristen for tilbyders krav går ut eller fordringen

av andre grunner ikke lenger kan inndrives, for eksempel ved foreldelse[66]. Kommunikasjonsformålet vil sjelden gi en lengre lagrinsadgang enn fakturaformålet. Når det gjelder telefoni, vil opplysninger som kan lagres til faktureringsformål således gi den lengste lagringsadgangen.

Konsesjonen etter personopplysningsforskriften[67] får betydning både for "trafikkdata" og andre "personopplysninger"[68]. Etter datatilsynets standard konsesjon for tilbydere av teletjenester[69] oppstilles en absolutt frist som er avhengig av faktureringshyppigheten. Denne fristen er på 3 eller 5 måneder ved henholdsvis månedsvis og kvartalsvis fakturering, se konsesjonsens punkt 8 "slettefrist". Denne absolutte frist kan fravikes dersom det har oppstått tvist mellom tilbyder og bruker, eller hvis faktura står ubetalt ved den normale frists utløp. Da gjelder en utvidet frist for lagring inntil tvisten er rettslig avgjort eller fakturaen betales. Dette følger også av konsesjonens punkt 8.

I prinsippet skal altså de loggførte data slettes så snart de ikke lenger er "nødvendige" for tilbyderen, eller uansett når det har gått 3 eller 5 måneder siden telefon- eller internettrafikken fant sted.

Når det gjelder opplysninger vedrørende internettjenester over bredbånd er omfanget av opplysninger som er "nødvendige" for faktureringsformålet mindre[70], slik at opplysninger om bruk av denne type tjenester som utgangspunkt skal slettes straks de ikke lenger er nødvendige for kommunikasjonsoverføring, jf. personopplysningsloven § 28 og ekomloven § 2-7, annet ledd.

---

[66] Se ot.prp. nr. 58 (2002-2003) s. 92

[67] § 7-1

[68] Jf. punkt 2.4.3

[69] Jf. personopplysningsforskriften § 7-1 jf. personopplysningsloven § 31, 4. ledd

[70] Se punkt 3.3.2

I denne sammenheng har datatilsynet overfor tilbydere i bransjen gjort prinsipielle vedtak angående lagring av opplysninger som kobler IP-adresser til brukerne av disse[71]. For opplysninger som angir hvilken abonnent som har fått tildelt hvilken IP-adresse til hvilken tid, fastsettes en absolutt frist som vil gjelde alle tilbydere av internettjenester. Fristen er satt til tre uker, men også her gjelder en kortere relativ frist etter nødvendighetsprinsippet.

Her ser vi sammenhengen til avhandlingens kapittel 5 om formålsendring. Med kriminalitetsbekjempelse som formål også i norsk lovgivning ville hele nødvendighetsdrøftelsen under dette kapittelet blitt en annen. Da kunne tenkes en mye lengre lagringsadgang, hvor hensyn også ble tatt til mulighetene for å løse straffesaker. Slik er ikke norsk lov utformet idag.

6.3 Endring/sammenligning

En minimumsendring av norsk lov etter Direktivet innebærer en utvidelse til seks måneders lagringstid.

Denne endringen må lovfestes, først og fremst i ekomloven, men også i personopplysningsloven dersom bestemmelser om innholdet i lagringsplikten gjennomføres her. Begge lover må få en bestemmelse som angir at de angitte opplysningene skal lagres i seks måneder.

For informasjon om en brukers mobil- og fasttelefoni har vi sett at dagens lovverk tillater lagring i inntil fem måneder ved kvartalsvis fakturering, dersom lagring av opplysningene er nødvendig for faktureringen. I disse tilfellene innebærer ikke en implementering av datalagringsdirektivet store endringer. Ved kvartalsvis fakturering vil det skje en utvidelse

[71] Se brev fra Datatilsynet til IKT-Norge av 13. mai 2009

av lagringstid fra maksimalt tre måneder til seks måneder. Dette vil være en dobling av lagringstiden, noe som ikke er ubetydelig.

For opplysninger som etter personopplysningsloven og ekomloven raskt skal slettes fordi de ikke er ”nødvendige” for faktureringsformålet, innebærer direktivet en betydelig utvidelse av lagringstid. Her nærmer vi oss drøftelsen om innføring av lagringsforpliktelse i kapittel 4. Dette gjelder blant annet opplysninger om mobiltelefonens lokasjon ved oppringninger, jf. datalagringsdirektivet art. 5 nr. 1 f) 1).

Når det gjelder internettilgang, er det særlig utvidelsen av lagringstid for IP-adresser som er relevant. Ellers vil endringene tilknyttet internettbruk stort sett falle inn under kapittel 4 om innføring av lagringsplikt.

7 Hvordan stiller endringene seg til menneskerettighetene?

7.1 Menneskerettsloven og Den Europeiske Menneskerettighetskonvensjon

For å kunne ta stilling til datalagringsdirektivets forhold til personvernreglene, må en ta utgangspunkt i bestemmelsene i Den Europeiske Menneskerettskonvensjon[72]. Gjennom menneskerettsloven av 21. mai 1999 nr. 30, er EMK gjort til norsk rett, se lovens § 2 nr. 1.

Ved lovens § 3 er konvensjonen gitt semikonstitusjonell rang. Det innebærer at dersom EMK strider mot annen formell norsk lov, skal dens bestemmelser gis forrang. Som vi skal se, innebærer imidlertid EMK art. 8, annet ledd at det ikke blir et spørsmål om rangsforholdet mellom de to regelsettene.

7.2 Artikkel 8 – Retten til respekt for privatliv

7.2.1 Innledning

EMK art. 8 regulerer den enkeltes rett til respekt for privatliv og familieliv:

> 1. Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.
>
> 2. Det skal ikke skje noe inngrep av offentlig myndighet i utøvelsen av denne rettighet unntatt når dette er i samsvar med loven og er nødvendig i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter.

Artikkelen innebærer en begrensning for reguleringer som går på bekostning av privatlivet til den enkelte. Bestemmelsens første ledd angir rettigheten, uten at dens innhold blir

[72] Heretter EMK

spesifisert nærmere. I annet ledd oppstilles "inngrepshjemmelen"[73]; det vil si i hvilke tilfeller et inngrep i denne rettigheten likevel kan tillates.

Først må det avgjøres om lagring etter datalagringsdirektivet omfattes av art. 8, første ledd. For å bestemme det nærmere innhold i EMK art 8, er praksis fra den europeiske menneskrettighetsdomstol[74] relevant og viktig. Det foreligger ingen avgjørelser i EMD som avgjør lovligheten av datalagringsdirektivets bestemmelser. Derfor må vi trekke slutninger fra øvrig praksis fra domstolen. EMD har gitt første ledd et vidtrekkende innhold, der overvåkning av offentlige og private registre over intime og fortrolige opplysninger omfattes[75]. Overvåkning av enkeltpersoner kan altså bryte med retten til privatliv etter art. 8 første ledd. Retten til respekt for ens korrespondanse er særskilt nevnt her. Bruk av telefon og internett inngår i dette begrepet[76].

Etter EMDs praksis er avlytting av enkeltindividers telefon klart inngrep i retten til privatliv og korrespondanse. Dette følger av EMD Klass and Others v Germany 1978. Men også registrering av hvilke telefonnumre som er ringt, når kommunikasjonen har skjedd og hvor lenge den har vart, bryter med denne rettigheten, jf. EMD Malone v the United Kingdom 1984. Domstolen kom i denne saken frem til at teleselskapet ikke hadde hatt rett til å gi slik teknisk informasjon videre til myndighetene. Begrunnelsen for dette var imidlertid at loven som hjemlet et slik inngrep ikke var tilstrekkelig presis eller tilgjengelig. Poenget er uansett at registrering av slike opplysninger er et inngrep som faller inn under EMK art. 8, første ledd.

Det er etter dette ingen tvil om at lagring av opplysninger som datalagringsdirektivet omhandler omfattes av EMK art. 8, første ledd.

---

[73] Høstmælingen (2003) s. 216

[74] Heretter EMD

[75] Høstmælingen (2003) s. 216

[76] Se EMD Klass and Others v Germany 1978 og Høstmælingen (2003) s. 229

Inngrepshjemmelen i art. 8, annet ledd angir de tilfeller hvor inngrep i retten til privatliv og familieliv rettferdiggjøres. Vilkårene er at det anses ”nødvendig i et demokratisk samfunn”, ”for the prevention of disorder or crime”. I tillegg gjelder et lovkrav, det vil si at inngrepet må være hjemlet i lov. Der et inngrep i privatlivet gjøres etter lov og med hensikt å forhindre kriminalitet, skjer det altså ikke brudd med rettigheten som følger av art. 8, første ledd, så fremt tiltaket er ”nødvendig i et demokratisk samfunn”.

Spørsmålet i denne avhandlingen blir dermed hvorvidt inngrepene likevel lar seg rettferdiggjøre etter artikkelens annet ledd. For at dette skal kunne skje, må for det første de lovregler som gis for å oppfylle direktivet være presise og tilgjengelige, slik at det ikke blir et spørsmål om dette som i EMD Malone v the United Kingdom 1984. Norske lovgivere må derfor sørge for at de nye reglene som angir lagringsplikten blir tilstrekkelig klare. Videre skal inngrepet skje av hensyn til et av artikkelens nevnte formål. Ettersom datalagringsdirektivet skal bekjempe kriminalitet[77], er dette vilkåret er oppfylt.

Dermed blir hovedproblemstillingen hvorvidt de inngrep direktivet innebærer er ”nødvendig i et demokratisk samfunn”.

I denne drøftelsen har EMD stilt opp et proporsjonalitetsprinsipp mellom mål og midler. I dette forholdsmessighetsprinsippet ligger at det ikke kan kreves at inngrepet er absolutt nødvendig, men det er heller ikke tilstrekkelig at tiltaket er ønskelig eller nyttig[78]. Det må foreligge et kvalifisert behov for å innføre datalagringsdirektivets regler med kriminalitetsbekjempelse som begrunnelse. Samtidig innebærer proporsjonalitetsnormen at jo mer alvorlig kriminalitet som skal bekjempes, jo større inngrep kan tåles. ”Jo mer langtrekkende inngrep eller jo mer alvorlig rett det gripes inn i, jo grundigere vil proporsjonalitetstesten være”[79]. Hvor ”grov kriminalitet” bekjempes kan altså mer krenkende tiltak godtas enn dersom det er tale om bekjempelse av mer ”ordinær” form for

[77] Jf. art. 1 nr. 1

[78] Se NOU 2004:6 s. 39

[79] Høstmælingen (2003) s. 232

kriminalitet. Opplysninger lagret med hjemmel i datalagringsdirektivet skal kun benyttes til bekjempelse av "grov kriminalitet", jf. art. 1, første ledd. Dette innebærer at det settes en lavere terskel for hvilke inngrep som kan rettferdiggjøres.

Statene er gitt en viss skjønnsmessig margin når det gjelder hvorvidt et inngrep er lovlig. Dette følger blant annet av EMD Handyside v the United Kingdom 1976, se para 48 og 49.

Problemstillingen vurderer jeg konkret i forhold til avhandlingens fire problemstillinger. I punkt 7.2.2 drøfter jeg om direktivets innføring av lagringsplikt er et inngrep som kan tillates etter EMK art. 8, annet ledd. Denne drøftelsen blir det nødvendig å knytte opp mot endringene i lagringens omfang. Under punkt 7.2.3 ser jeg på det samme spørsmålet når det gjelder formålsendringen etter datalagringsdirektivet art. 1 nr. 1. Hvorvidt direktivets regler om lagringstid kan begrenses av personvernregelen drøfter jeg i punkt 7.2.4.

7.2.2 Overgangen til lagringsplikt

7.2.2.1 Innledning

Spørsmålet er her om en innføring av lagringsplikt, jf. kapittel 4 ovenfor, er "nødvendig i et demokratisk samfunn" for bekjempelse av kriminalitet. Dersom lagringplikten ikke er "nødvendig", vil en bestemmelse som pålegger tilbyderne å loggføre dataopplysninger være i strid med enkeltindivitets rett til "respekt for sitt privatliv", jf. EMK art. 8.

Proporsjonalitetsprinsippet[80] innebærer en drøftelse av inngrepets rekkevidde og menneskeretten det gjøres innhugg i. Er et inngrep av denne typen, hvor det lagres opplysninger om hvor og når kunden har benyttet seg av internett eller telefon og til hvem kommunikasjonen skjer, et meget alvorlig inngrep eller et mindre alvorlig inngrep? For å kunne besvare spørsmålet om hvorvidt datalagringsdirektivet er "nødvendig i et

[80] Jf. ovenfor punkt 7.2.1

demokratisk samfunn", må drøftelsen av inngrepets alvorlighetsgrad foretas i forhold til de ulike opplysningene datalagringsdirektivet innebærer lagringsplikt for.

7.2.2.2 Telefoni

Når det gjelder telefoni, innebærer datalagringsdirektivet enkelte endringer når det gjelder lagring. Etter datalagringsdirektivet art. 5 nr. 1 b) 1) ii) skal navn og adresse til mottaker av telefonsamtale heretter lagres. Det skjer allerede lagring av mottakernes telefonnummer jf. ekomloven § 2-7, da disse opplysningene anses som "nødvendige" for fakturaformål[81]. Sammenholdt med at navn og adresse til abonnenten av dette nummeret stort sett er tilgjengelig informasjon for påtalemyndigheten (som er de som skal ha innsyn i tilbyders logger), må det konkluderes med at denne endringen ikke innebærer et alvorlig inngrep i vernet av den personlige frihet. Dermed stilles ikke høye krav før en kan godta at slike opplysninger lagres, jf. proporsjonalitetsprinsippet i EMK art. 8, annet ledd. Er det "nødvendig" med opplysninger om navn og adresse til mottaker av telefonsamtaler for å bekjempe grov kriminalitet? Informasjonene gjør en oppsporing enklere. Samtidig er disse opplysningene allerede tilgjengelig på annet vis, slik at en lagring av disse dataene hos tilbyder kun forenkler en sporingsprosess for påtalemyndighetene. Dermed vil denne loggføringen bli veldig nærme det "ønskelige". Ettersom dette er på grensen til i det hele tatt å kalles et inngrep, må imidlertid lagring av mottakers navn og adresse trolig være greit.

De samme tankene må gjøre seg gjeldende for opplysninger om mottakerens IMSI/IMEI-nummer, som skal lagres etter datalagringsdirektivet art. 5 nr. 1 e) 2), slik at også lagring av disse data må godtas som lovlige inngrep.

At det ved en implementering av datalagringsdirektivet skal lagres data som angir lokalisering av brukeren via celle-ID, jf. datalagringsdirektivet art. 5 nr. 1. f) 1), innebærer den største endringen for mobiltelefonbrukeren. Ved innsyn i tilbyders logger kan en

[81] Se punkt 3.2.2.2 ovenfor

heretter angi i hvilke områder brukeren har befunnet seg mens telefonen hans har vært i bruk. Er dette et alvorlig inngrep? Dette er nok i kjernen av den personlige frihet som skal vernes, og minner om overvåking, og vi befinner oss i grenseland til det som må betegnes som ulovlige inngrep i personvernet. Dermed må det stilles veldig høye krav for nødvendigheten av disse opplysningene i en kriminalitetsbekjempende prosess. Inngrep av denne sorten vil riktignok kun skje overfor en "mistenkt" eller "siktet"[82], og det må legges til grunn at påtalemyndighetene fremdeles må grunngi utleveringskrav. Det er ikke snakk om å utlevere opplysninger knyttet til en hvilken som helst bruker. Samtidig kan det være av stor betydning å kunne plassere en mistenkt i området for forbrytelsen ved hjelp av celle-ID. Det må imidlertid også fastslås hvem som har vært bruker av telefonen på tidspunktet, noe som ikke alltid like enkelt. Dette er et krav som rettferdiggjør utleveringen. Derfor konkluderer jeg med at innholdet i datalagringsdirektivet art. 5 nr. 1 f) 1) ikke bryter med EMK art. 8, og kan dermed gjennomføres i norsk rett.

7.2.2.3 Internett

Når det gjelder internett vil datalagringsdirektivet innebære flere endringer i data som skal loggføres av tilbyder.

En av endringene er at det heretter skal lagres hvilken kommunikasjonstype brukeren har benyttet, jf. datalagringsdirektivet art. 5 nr. 1 d) 2), det vil si hvorvidt brukeren har benyttet internett til bruk av e-postforsendelse eller IP-telefoni. Er dette et alvorlig inngrep? Tilfellet ligger nok i det nedre skiktet når det gjelder alvorlighetsgrad. Det samme når det gjelder nødvendighet. Jeg er tilbøyelig til å godta lagring av kommunikasjonstype etter EMK art. 8, annet ledd.

Når det etter datalagringsdirektivet skal lagres hvem som er mottaker av e-postforsendelse eller telefonsamtaler over internett, har vi med en større endring å gjøre, og det må også spørres om dette er et alvorlig inngrep. Dette er trolig et inngrep som ligger høyere på

[82] Jf. kapittel 5

skalaen, og hvor det må kreves at lagringen er nærmere det uunnværlige. Er disse opplysningene viktige for å løse kriminalsaker? Med hensyn til for eksempel barneporno kan være av høy viktighetsgrad å kunne spore mottaker av e-post med ulovlig innhold. Denne er muligens også er en del av et større nettverk som det er viktig å få stanset. Det samme må anføres også overfor andre grove forbrytelser. Det må derfor anses som "nødvendig i et demokratisk samfunn" å lagre slike opplysninger, slik at lagringsplikten ikke heller her medfører brudd på EMK art. 8.

Neste spørsmål er hvorvidt lagring av tidspunkt for inn- og utlogging fra e-post og telefoni via internett er et alvorlig inngrep. Dette er data som kan hjelpe til med å fastslå når brukeren har benyttet seg av telefoni eller internett. Jeg vil si at lagring av slike opplysninger hverken er et meget alvorlig eller et mindre alvorlig inngrep. Spørsmålet blir, er det "nødvendig i et demokratisk samfunn"? David Toska ble etter NOKAS-ranet pågrepet i Spania som følge av pålogging til sin private mail fra samme IP-adresse. Koblet sammen med lagrede IP-adresser, har det altså vist seg å være nødvendig for å bekjempe alvorlig kriminalitet. Jeg konkluderer derfor med at heller ikke lagring av tidspunkt for inn- og utlogging fra e-post og telefoni via internett bryter med EMK art. 8.

Når det gjelder lagring av dato, klokkeslett og varighet for bredbåndsabonnenters bruk, vil jeg si at det neppe er et kjempealvorlig inngrep i den personlige frihet. Det kan nok være til hjelp i oppklaringen av en straffesak å kunne fastslå når bredbåndsabonnenten har vært tilkoblet internett. Derfor må også denne form for datalagring godtas.

Det har tidliger vist seg svært nyttig for påtalemyndigheten å kunne ha tilgang til slike logger som datalagringsdirektivet art. 5 gir hjemmel for. Blant annet Nokas-saken, Lommemannen-saken, Orderud-saken og Baneheia-saken. Dette er uomtvistelig saker som må karakteriseres som forbrytelser av alvorlig art, hvor det har vært viktig å finne bakmennene.

Jeg har konkludert med at lagring av celle-ID, jf. datalagringsdirektivet art. 5 nr. 1 f) 1), trolig medfører brudd på EMK art 8. Dermed kan bestemmelsen ikke gjennomføres i norsk rett.

De øvrige delene av datalagringsdirektivet art. 5 kan gjennomføres i norsk rett uten at vi bryter med menneskerettighetene.

7.2.3 Formålsendring

Som vi så i kapittel 5 innebærer datalagringsdirektivet at de lagrede opplysningene skal kunne benyttes til å bekjempe kriminalitet, og ikke lenger for faktura- og kommunikasjonsformål, jf. ekomloven § 2-7, annet ledd og personopplysningsloven § 28. Jeg konkluderte med at det kun blir en endring dersom en tolker ”detection” slik at direktivet innebærer en generell innsynsrett overfor de lagrede data, men at en slik tolking er tvilsom.

Utenfor disse tilfellene kan det vanskelig reises en problemstilling om brudd på retten til respekt for privatlivet. Det er nettopp kriminalitetsbekjempelse som legitimerer inngrep i denne menneskeretten, jf. EMK art. 8, annet ledd. Lagring av trafikkdata får ved datalagringsdirektivet et stødigere grunnlag overfor menneskerettighetene.

Spørsmålet om datalagringsdirektivet bryter med personvernreglene blir derfor kun aktuelt i forhold til ”detection”-drøftelsen. Inngrepet her vil være at det skjer en form for generell innsynsrett i registre tilknyttet telefon- og internettbrukerne i Norge, uten konkret mistanke, slik det idag kreves etter straffeprosesslovens regler. Påtalemyndighetene får hjemmel til å gjennomføre kontrollsjekker av tilfeldige brukeres telefoni eller internettbruk for å sjekke om det foregår kriminell atferd. Om dette vil skje, er et annet spørsmål. Når en ser på politiets overfylte agenda, er det lite trolig at de vil bruke tid på å sjekke brukere som ikke kan knyttes til en kriminell handling. Det som derimot kan tenkes, er at påtalemyndighetene bruker en slik bestemmelse til å sjekke trafikkdata mot en person hvor det ikke etter dagens regler er tilstrekkelig hjemmel til å få innsyn. Ved innføring av en slik

”overvåkingsbestemmelse” risikerer vi med andre ord å få en innsynshjemmel uten begrunnelse, uten vilkår og uten kontrollmuligheter.

Dersom en kommer til at ”detection” innebærer en slik hjemmel, får vi et meget alvorlig inngrep som må ligge tett opptil det absolutt nødvendige for å godtas. Det gjør ikke en slik form for innsynsrett. Det kan derfor ikke gjennomføres en regel i norsk rett som innebærer en slik tolking av ”detection”, da det vil bryte med EMK art. 8.

7.2.4 Endring i lagringstid

Lagringstiden til data som skal lagres utvides ved datalagringsdirektivet til minimum 6 måneder, jf. datalagringsdirektivet art. 6, fra en periode som idag avgjøres ut i fra nødvendighet for fakturering, jf. ekomloven § 2-7, annet ledd og personopplysningsloven § 28. Som kapittel 6 i avhandlingen viste, er utvidelsen av varierende grad, ettersom hvilke opplysninger det er tale om.

Problemstillingen her dreier seg om opplysninger som allerede lagres idag, ikke opplysninger som datalagringsdirektivet innebærer en innføring av lagring for. Denne drøftelsen har jeg foretatt ovenfor under punkt 7.2.2.

Når det gjelder telefoni, innebærer datalagringsdirektivet en utvidelse i lagringstid fra 3 eller 5 måneder, til 6 måneder. Ved å utvide med en måned vil ikke inngrepet i personvernet bli meget større. Det kan i vårt tilfelle ikke tenkes at en ved dette kommer over en terskel som innebærer brudd med EMK art. 8. Når enkelte rammes av en utvidelse til det dobbelte, fra 3 måneder til 6 måneders lagring, kan det virke mer betydelig. Det er imidlertid de samme opplysningene det gjelder, slik at dersom en lagringsutvidelse fra 5 til 6 måneder godtas, må det samme være tilfelle ved en utvidelse fra 3 til 6 måneder.

Ved internettbruk ble spørsmålet om endring av lagringstid særlig aktuelt ved lagring av IP-adresser[83]. Datalagringsdirektivet vil her innebære en endring fra 3 uker til 6 måneder. Dette er en betydelig utvidelse, som omfatter inngrep etter EMK art. 8, første ledd. Det må da spørres om det er nødvendig å utvide lagringstiden på en så omfattende måte. Ettersom straffeprosessloven innebærer at det stilles krav om en spesiell mistenkt for å få innsyn[84], kan det ta tid før påtalemyndighetene kommer til et stadie hvor de har grunnlag for å kreve opplysninger utlevert fra tilbyder. Oppklaringstiden for grov kriminalitet kan være lang, og en tidsfrist på 3 uker for innsyn i opplysninger som kan være ledd i kriminaliteten vil være totalt urealistisk. Datalagringsdirektivet art. 6 kan virke som en overdreven utvidelse, men sett i sammenheng med reglene om foreldelse for grov kriminalitet[85], kan lagring i en periode på 6 måneder være greit. Jeg konkluderer med at datalagringsdirektivets bestemmelse om lagringstid ikke bryter med EMK art. 8.

Ved å ha en kort tidsfrist for sletting av IP-adresser, kan Norge bli et yndet tilholdssted for kriminelle som ønsker å unngå å rammes av lagringstiden som gjelder i store deler av Europa. Dette bør unngås.

[83] Se ovenfor punkt 6.3

[84] Se punkt 5.2.2 ovenfor

[85] Se strl. §§ 67-69

8 Avslutning/konklusjon – Forslag til endringer i Norsk lov

Vi har sett at datalagringsdirektivet vil innebære at det må skje endringer i de reglene vi finner i ekomloven og personopplysningsloven idag. De mest omfattende endringene vil gjelde lagringsplikt for data knyttet til internettbruk, men også lokaliseringsdata for mobiltelefoni omfattes.

Spørsmålet jeg reiste innledningsvis er hvilken fremgangsmåte som lønner seg for å gjennomføre disse endringene i norsk rett.

En egen lov som gjengir innholdet av datalagringsdirektivet, vil innebære endel dobbeltreguleringer innenfor rettsområdet. Det mest elegante er at hele regelverket er i samsvar, og dermed vil det også ved en slik gjennomføringsmåte måtte skje endringer i ekomloven og personopplysningsloven. Dette kan gjøres enkelt, ved for eksempel en bestemmelse som angir at den nye ”datalagringsloven” går foran i tilfellle motstrid. Datalagringsdirektivets krav kan imidlertid også tenkes oppfylt ved endringer direkte i personopplysningsloven og ekomloven. Da bør samtidig forholdet disse to lovene imellom klargjøres. Problemstillingen blir hva som er mest ryddig og oversiktlig, og samtidig hva som sikrer at alle regler i datalagringsdirektivet blir gjennomført slik de skal.

I datalagringsdirektivet art. 5 finner vi en omfattende opplisting av de opplysninger som skal lagres etter direktivet. Denne bestemmelsen bør gjengis ordrett i norsk rett, slik at alle de nevnte data blir gjenstand for lagring også her. Dette blir en meget omfattende regulering å gi plass i ekomloven § 2-7, annet ledd. Derfor bør, etter mitt syn, hele art. 5 i datalagringsdirektivet vies en egen lovbestemmelse.

Selve lagringsforpliktelsen[86] kan innlemmes i den samme bestemmelsen som angir innholdet av lagringsplikten[87] Det samme gjelder reguleringen av lagringstid[88]. Formålsangivelsen har vi sett at det ikke er strengt nødvendig å lovfeste i norsk rett. Dermed står vi igjen med behov for kun én bestemmelse, som er nok til å sørge for at Norges minimumsforpliktelser etter direktivet oppfylles.

Det kan sees som forholdsvis unødvendig å gi en egen "datalagringslov", der det kun er nødvendig med en enkelt bestemmelse, selv om denne vil bli forholdsvis omfattende. Bestemmelsen bør komme i ekomloven, ettersom det vil gi den mest naturlige sammenhengen i regelverket, jf. drøftelsen i punkt 2.4.3. Ved denne gjennomføringsmåten omfattes både juridiske og fysiske brukere, uten den begrensning personopplysningsloven har[89]. Her bør lagringsforpliktelsen oppstilles, med det nærmere innhold denne skal ha, jf. datalagringsdirektivet art. 5, samt den lagringstid Norge velger å innføre, jf. datalagringsdirektivet art. 6.

Hva bør videre skje med ekomloven § 2-7, annet ledd? Den må i stor grad fjernes slik den er idag. En endring kan tenkes, og bør nok foretrekkes. Det bør opprettholdes en sletteplikt fra det tidpunktet lagringstiden etter datalagringsdirektivet utløper. Dette for å unngå at tilbyder unnlater å slette loggene sine når maksimal lagringstid er utløpt. En lagringstid utover Norges minimumsforpliktelse kan muligens bryte med personvernet i EMK art. 8. Samtidig bør det fremdeles åpnes for en ytterligere lagringsadgang i fakturaøyemed. Det kan tenkes tvister rundt brukerens skyldige beløp, og derfor må tilbyder kunne lagre data som knytter seg til abonnentens bruk til dette er gjort opp, slik norsk lov åpner for idag[90]. I disse tilfeller må nødvendighetsvilkåret opprettholdes som grunnlag for lagring.

---

[86] Jf. datalagringsdirektivet art. 3

[87] Jf. datalagringsdirektivet art. 5

[88] Jf. datalagringsdirektivet art. 6

[89] Jf. ekomloven § 1.5 nr. 12 og personopplysningsloven § 2 nr. 1

[90] Jf. punkt 6.2 ovenfor

Vi har også sett at ingen av bestemmelsene i datalagringsdirektivet må utelates på grunn av personvernregelen i EMK art. 8. EMK art. 8 stenger imidlertid for en tolking av ordet ”detection” i datalagringsdirektivet art. 1 slik at påtalemyndighetene får en generell tilgang til de lagrede register[91]. Et krav om å kunne knytte opplysninger til en konkret mistenkt og en konkret hendelse må opprettholdes i straffeprosessen.

Det er hensynet til personvern og til teleselskapene som etter dagens lovgivning avgjør om lagring av trafikkdata skal skje. Lovgivningen tar ikke hensyn til bekjempelse av kriminalitet. Med omfattende og ekspanderende kriminalitet i det norske samfunnet, er ikke dette et riktig utgangspunkt å ha i norsk rett. Det kan derfor hevdes at datalagringsdirektivet innebærer en forbedring i norsk rettstilstand.

[91] Se punkt 7.2.3 ovenfor

9 Litteraturliste

Litteratur

Andenæs, Johs. *Alminnelig strafferett.* 5. utgave, Oslo, 2004

Eckhoff, Torstein *Rettskildelære.* 5. utgave, Oslo, 2001

Hov, Jo *Rettergang I.* Oslo, 2007

Hov, Jo *Rettergang II.* Oslo, 2007

Høstmælingen, Njål *Internasjonale menneskerettigheter*. Oslo, 2003

Schartum, Dag Wiese og Bygrave, Lee A. *Personvern i informasjonssamfunnet.* Bergen, 2004

Ordboka

EU-direktiv

EP/Rdir 95/46 EF	Europaparlaments- og rådsdirektiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger
EP/Rdir 97/66 EF	Europaparlaments- og rådsdirektiv 97/66/EF av 15. desember 1997 om behandling av personopplysninger og beskyttelse av privatlivets fred innenfor telesektoren

EP/Rdir 2002/58 EF	Europaparlaments- og rådsdirektiv 2002/58/EF av 12. juli 2002 om behandling av personopplysninger og personvern i sektoren for elektronisk kommunikasjon
EP/Rdir 2006/24 EF	Europaparlaments- og rådsdirektiv 2006/24/EF av 15. mars 2006 om lagring av data generert eller behandlet i forbindelse med tilveieblivelse av offentlig tilgjengelige elektroniske kommunikasjonstjenester eller elektroniske kommuniasjonsnett og om endring av direktiv 2002/58/EF

Traktater

EMK	Den europeiske menneskerettighetskonvensjon, Roma 1950
EF-traktaten	Traktaten om opprettelse av Det europeiske fellesskap, Roma 1957
EØS-avtalen	Avtale om Det europeiske økonomiske samarbeidsområde, 1994

Lover

Grunnloven av 17. mai 1814

Almindelig borgerlig Straffelov (straffeloven) av 22. mai 1902 nr. 10

Lov om rettergangsmåten i straffesaker av 22. mai 1981 nr. 25

Lov om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS) m.v. (EØS-loven) av 27. november 1992 nr. 109

Lov om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven) av 21. mai 1999 nr. 30

Lov om behandling av personopplysninger av 14. april 2000 nr. 31

Lov om elektronisk kommunikasjon (ekomloven) av 4. juli 2003 nr. 83

Forskrifter

FOR 2000-12-15 nr 1265:	Forskrift om behandling av personopplysninger (personopplysningsforskriften)
FOR 2004-02-16 nr 401:	Forskrift om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften)

Rettspraksis

Handyside v. the United Kingdom	Case of Handyside v. the United Kingdom 1976-12-07 EMD (http://cmiskp.echr.coe.int/)
Klass and others v Germany	Case of Klass and Others v. Germany 1978-09-06 EMD, ECHR (http://www.echr.coe.int/echr/)
Malone v the United Kingdom	Case of Malone v. the United Kingdom 1984-02-08 EMD, ECHR (http://www.echr.coe.int/echr/)

Forarbeider

Ot.prp. nr. 64 (1998-1999)	Om lov om endringer i straffeprosessloven og straffeloven m.v.

Ot.prp. nr. 58 (2002-2003)	Om lov om elektronisk kommunikasjon (ekomloven)
NOU 2004: 6	Mellom effektivitet og personvern – Politimetoder i forebyggende øyemed
NOU 2009: 1	Individ og integritet – Personvern i det digitale samfunnet
NOU 2009: 15	Skjult informasjon – åpen kontroll

Alle disse opplysningene er å anse som ”trafikkdata”. Derfor må ekomloven få en bestemmelse som innebærer at brukeridentiteten til mottaker av e-post og IP-telefonsamtaler, opplysninger om kommunikasjonstype, tidspunkt for inn- og utloggen av e-post og IP-telefoni skal lagres.

Andre kilder

Brev fra Datatilsynet til IKT-Norge 2009 (sitert september 2009) (http://www.datatilsynet.no/upload/tilsynsrapporter/2008/Microsoft Word - 09-00699-1 Lagring av IP-adresse og abonnement.pdf)

A